HACKING THE HOMELAND: INVESTIGATING CYBERSECURITY VULNERABILITIES AT THE DEPARTMENT OF HOMELAND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JUNE 20, 2007

Serial No. 110–52

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
48–926 PDF WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

JAMES R. LANGEVIN, Rhode Island, *Chairman*

ZOE LOFGREN, California
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
AL GREEN, Texas
VACANCY
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

MICHAEL T. MCCAUL, Texas
DANIEL E. LUNGREN, California
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
PETER T. KING, New York *(Ex Officio)*

JACOB OLCOTT, *Director & Counsel*
DR. CHRIS BECK, *Senior Advisor for Science & Technology*
CARLA ZAMUDIO-DOLAN, *Clerk*
DR. DIANE BERRY, *Minority Senior Professional Staff Member*

CONTENTS

HACKING THE HOMELAND: INVESTIGATING CYBERSECURITY VULNERABILITIES AT THE DEPARTMENT OF HOMELAND SECURITY

Wednesday, June 20, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY,
AND SCIENCE AND TECHNOLOGY,
Washington, DC.

The subcommittee met, pursuant to call, at 2:20 p.m., in Room 311, Cannon House Office Building, Hon. James R. Langevin [chairman of the subcommittee], presiding.

Present: Representatives Langevin, Lofgren, Christensen, Etheridge, Thompson, ex officio, McCaul, and Brown-Waite.

Mr. LANGEVIN. The subcommittee will come to order. The subcommittee's meeting today is to receive testimony on Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security.

Ladies and gentlemen, good afternoon. I want to thank the witnesses for appearing before the subcommittee, and we look forward to your testimony today. The Internet has brought our friends close and our enemies closer. As each day passes, another incident reminds us that our information and our IT infrastructures are vulnerable.

Cases in point: Estonia, a technically savvy country, was brought to its knees by hackers who took down government Web sites.

The Pentagon recently asserted that China is developing viruses to attack computer systems to obtain electromagnetic dominance early in a conflict.

The incident formerly classified as Titan Rain suggested that the Chinese have been coordinating attacks against the Department of Defense networks for years.

This subcommittee has been holding a series of hearings on cybersecurity, and it has become very clear the infiltration of Federal Government networks and the possible theft or exploitation of our information is one of the most critical issues confronting our Nation today.

In April, the subcommittee discussed a series of attacks penetrated by hackers—perpetrated by hackers operating through Chinese Internet servers against computer systems at the Departments of Commerce and State. Hackers were able to penetrate Federal systems and use "rootkits," a form of software that allows attackers to mask their presence, to send information back out of

our own systems. At the time, I was critical of the security efforts at both State and Commerce, but assured them that I would be posing the same kinds of questions about network security to DHS. Well, that is why we are here today.

It was actually a shock and a disappointment to learn that the Department of Homeland Security, the agency charged with being the lead in our national cybersecurity, has suffered so many significant cybersecurity incidents in its own networks. It is equally disturbing that the Department is so slow to respond to fixing these problems.

DHS reported to the committee that it experienced 844 cybersecurity incidents in fiscal years 2005 and 2006. These incidents occurred on IT networks at DHS headquarters, ICE, CBP, FEMA and others. I would like to take a minute to share a few representative incidents of what I am talking about:

A password dumping utility and other malicious files were found on two DHS systems.

Computers contained suspicious beaconing activity and an IRC bot, which is a generic detection for a group of backdoor Trojan horses that allows a hacker to control the compromised computer.

Workstations infected with multiple Trojans and viruses.

The user ID and passwords for a local administrator were found in hard copy.

A Department Web site has been compromised.

Classified e-mails were sent over unclassified networks.

A workstation was infected with a Trojan scanning for port 137, an event that clearly demonstrated individuals attempting to scan DHS systems through the Internet.

Unauthorized software was installed on an asset that could allow security settings circumvention.

Unauthorized users had been attaching their personal computers to DHS networks.

Unauthorized individuals gained access to DHS equipment and data.

Firewalls had been misconfigured by a contractor to allow all ICMP traffic to and from the Internet.

And there had been numerous classified data spillages, according to our reports.

I am going to stop there. Each of these incidents that I have just mentioned represents a significant security breach. Some of these incidents are the result of blatant disregard by DHS IT policy, and I hope that those responsible have been properly disciplined. But others are reminiscent of classic attack patterns by formidable adversaries

We saw these exact incidents on State Department and Commerce Department computers several months ago. These aren't just my conclusions. In spite of some of the significant vulnerabilities in its systems, the Department doesn't appear to be in any rush to fix them.

Now, According to the September 2006 DHS IG report on DHS information systems, 69 percent of the 3,566 open vulnerabilities that existed on the Department's networks did not include the resources required for remediating those vulnerabilities. In fact, some of the agencies aren't even reporting incidents to the DHS Com-

puter Security Incident Response Center, CSIRC, as required by law.

These components apparently don't understand that vulnerabilities on their individual systems can affect the entire Homeland Security network. Furthermore, information provided by DHS suggests that the CIO is failing to engage in best defense practices that would limit penetrations into DHS networks. DHS does not conduct rogue tunnel audits, ingress/egress filtering on DHS personal computers, widespread internal and external penetrations tests on its systems, audits on IT contractors. DHS hasn't mandated two factor authentication across the Department, which would demonstrate what types of critical vulnerabilities remain on DHS networks. How can DHS be the Nation's and the government's cybersecurity leader with this kind of a track record?

The fact is, DHS is failing to dedicate adequate funding to network security. The finances show that Mr. Charbo and the Department's leadership continue to underinvest in IT security. Mr. Charbo cut funding for the chief information security officer and only slightly increased the IT security budget. Experts agree that agencies should allocate around 20 percent of their IT budgets to cybersecurity, and yet DHS is only spending 6.8 percent to secure their systems. All of this is happening while the Department's IT budget was increased by $1 billion last year.

Unfortunately, the failure to invest in defensive measures and mitigate vulnerabilities is jeopardizing the Department's mission. That is not just my conclusion; that is the conclusion that the GAO reached in an upcoming report about the IT systems supporting US–VISIT. GAO will report that these IT systems are riddled with significant information security control weaknesses that place sensitive and personally identifiable information at increased risk of unauthorized disclosure and modification, misuse, and destruction, possibly without detection, and place program operations at increased risk of disruption.

What does all of this mean? It means that terrorists or nation-states could be hacking Department of Homeland Security databases, changing or altering their names to allow them access to this country, and we wouldn't even know that they were doing it. If we care about protecting our homeland from dangerous people, we have to care about the security of the information that we use to accomplish that mission.

I wish that DHS exerted the same level of effort to protect its networks that our adversaries are exerting to penetrate them. But as long as this striking and dangerous imbalance persists, the success of the Department's mission remains in serious doubt.

Again, I want to thank the witnesses for being here today. I look forward to probing these critical issues further.

[The statement of Mr. Langevin follows:]

PREPARED OPENING STATEMENT OF THE HONORABLE JAMES R. LANGEVIN, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

• Ladies and gentlemen, good afternoon. I thank the witnesses for appearing before the Subcommittee, and we look forward to your testimony.

• The Internet has brought our friends close and our enemies closer.

• As each day passes, another incident reminds us that our information and our IT infrastructures are vulnerable to attacks.
  • Estonia—a technologically savvy country—was brought to its knees by hackers who took down government websites.
  • The Pentagon recently asserted that China is developing viruses to attack computer systems to obtain "electromagnetic dominance early in a conflict."
  • The incident formerly classified as Titan Rain suggested that the Chinese have been coordinating attacks against Department of Defense networks for years.
  • This Subcommittee has been holding a series of hearings on cybersecurity, and it has become clear to me that the infiltration of federal government networks and the exfiltration of our information is one of the most critical issues confronting our nation.
• In April, the Subcommittee discussed a series of attacks perpetrated by hackers operating through Chinese Internet servers against computer systems at the Departments of Commerce and State.
• Hackers were able to penetrate Federal systems and use "rootkits"—a form of software that allows attackers to mask their presence—to send information back out of our systems.
• At the time, I was critical of the efforts by both State and Commerce, but assured them that I would be asking the same kinds of questions about network security to DHS.
• That's why we're here today.
• I am disappointed to learn that the Department of Homeland Security—the agency charged with being the lead in cybersecurity—has suffered so many significant security incidents on its networks. DHS reported to the Committee that it experienced *844* "cybersecurity incidents" in fiscal years 2005 and 2006. These incidents occurred on IT networks at DHS headquarters, ICE, CBP, FEMA, and others.
• I will share a few representative incidents:
  • A password dumping utility and other malicious files were found on two DHS systems.
  • Computers contained suspicious beaconing activity, an IRC bot, and other malware.
  • Workstations infected with multiple Trojans and viruses.
  • The User id and passwords for a local administrator account were found in hard copy.
  • A Department website has been compromised.
  • Classified emails were sent over unclassified networks.
  • A workstation was infected with a Trojan scanning for port 137.
  • Unauthorized software was installed on an asset that could allow security setting circumvention.
  • Unauthorized users have been attaching their personal computers to the DHS network
  • Unauthorized individuals gained access to DHS equipment and data.
  • Firewalls have been misconfigured by a contractor to allow all ICMP traffic to and from the Internet.
  • And there have been numerous "Classified data spillages"
• I'll stop there. Each of these incidents that I've just mentioned represents a *significant security breach.*
• Some of these incidents are the result of blatant disregard of DHS IT policy, and I hope that those individuals have been properly disciplined.
• But other incidents are reminiscent of classic attack patterns by formidable adversaries—we saw these *exact incidents* on State Department and Commerce Department computers several months ago.
• In spite of the significant vulnerabilities to its systems, the Department doesn't appear to be in any rush to fix them. According to the September 2006 DHS IG report on DHS information systems, 69% of the 3,566 open vulnerabilities that exist on the Department's networks did not include the resources required for remediating those vulnerabilities. In fact, some components aren't even reporting incidents to the DHS Computer Security Incident Response Center (CSIRC), as required by law.
• These components apparently don't understand that vulnerabilities on their systems can affect the entire Homeland Security network. Furthermore, information provided by DHS suggests that the CIO is failing to engage in defensive best practices that would limit penetrations into the DHS networks.
• DHS does not conduct rogue tunnel audits, ingress/egress filtering on DHS client personal computers, widespread internal and external penetration tests on his

systems, audits on IT contractors. DHS hasn't mandated two factor authentication across the Department.

• How can DHS be the cybersecurity leader with this track record? DHS is failing to provide adequate funding to network security.

• The finances show that Mr. Charbo and the Department's leadership continue to under-invest in IT security. Mr. Charbo cut funding for the Chief Information Security Officer and only slightly increased the IT security budget. All of this is done while the Department's IT budget was increased by $1 b last year.

• Unfortunately, the failure to invest in defensive measures and mitigate vulnerabilities is jeopardizing the Department's mission.

• That's the conclusion that the GAO reached in a report that they're about to release about the IT systems supporting US–VISIT.

• GAO will report that these IT systems are *"riddled with significant information security control weaknesses* that place sensitive and personally identifiable information at increased risk of unauthorized disclosure and modification, misuse, and destruction possibly without detection, and place program operations at increased risk of disruption."

• What does this mean?

• It means that terrorists or nation states could be hacking Department of Homeland Security databases, changing or altering their names to allow them access to this country, *and we wouldn't even know they were doing it.* If we care about protecting our homeland from dangerous people, we have to care about the security of our information that we use to accomplish the mission.

• I wish DHS exerted the same level of effort to protect its networks that our adversaries are exerting to penetrate them.

• But as long as the effort level remains imbalanced, the success of the Department's mission remains in doubt.

• This concludes my opening statement.

Mr. LANGEVIN. And at this time, the Chair now recognizes the ranking member of the subcommittee, the gentleman from Texas, Mr. McCaul, for the purpose of an opening statement.

Mr. MCCAUL. And I thank the chairman for holding this hearing on the state of information security at the Department of Homeland Security.

This is an issue of national security, and it is an issue that I am glad that you brought to the forefront. As we learned last month, our Federal systems are under attack on a near-constant basis. Viruses and spam are the least of our worries. There is evidence that organized, malicious hackers are targeting government systems, as well as those of government contractors. These attacks result in a truly frightening outflow of information from our departments and our Federal agencies, and the only way to counter these hackers is to improve our security posture and stay as vigilant and proactive as possible to counter them.

Unfortunately, outside hackers are not the only threats to our sensitive information. Malicious insiders, untrained users, and basic carelessness are also threats to the integrity of our networks. Information systems have become so pervasive and so complex that users have become a weak link in the security chain. End users of our systems need to receive proper security training, and security policies need to be clear and responsive.

The Department has had the challenge of putting together 22 different agencies and components, each with its own security policies and culture. No doubt this is a very tough job. I look forward to the testimony of Mr. Scott Charbo, the Chief Information Officer, who will testify on the challenges of combining the legacy system into a single system, and how he has designed the security program to protect the Department's networks and systems. And I

hope that the GAO will offer some constructive criticism and provide workable recommendations for the Department.

Beyond the operational responsibilities of Mr. Charbo, there are aspects of the Department's other cybersecurity programs I would like this subcommittee to investigate. Specifically, I am concerned that the Department may not be coordinating their efforts enough with private sector experts, and am interested to see how the Department has worked with the private sector to protect the country as a whole.

I would also like to see a report on what the Department has done and a road map for where it plans to go in the future.

Most importantly, I would like to see, and this is long overdue, a strategic national vulnerability assessment to be done on United States cybersecurity. This has never been done. It is long overdue, and the Nation deserves it, and the Nation needs this to protect it. I have said it before: I believe an attack on our information infrastructure could be worse than the effects of a weapon of mass destruction, and I would hope the Department would take it just as seriously.

Mr. Chairman, I hope the subcommittee can continue to assist the Department in its efforts to protect and secure this country's critical information infrastructure, and I yield back the balance of my time.

[The statement of Mr. McCaul follows:]

PREPARED OPENING STATEMENT OF THE HONORABLE MICHAEL T. MCCAUL, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

Thank you, Mr. Chairman. I appreciate you holding this hearing on the state of information security at the Department of Homeland Security. As we learned last month our federal systems are under attack on a near constant basis. Viruses and spam are the least of our worries. There is evidence that organized malicious hackers are targeting government systems as well as those of government contractors. These attacks result in a flow of information out of our Departments and Agencies that is truly frightening. The only way to counter these hackers is to improve our security posture, staying as vigilant and proactive as possible in order to take effective action to counter the effects of these hackers.

Unfortunately, outside hackers are not the only threats to our sensitive information, malicious insiders, untrained users and basic carelessness are also threats to the integrity of our networks. Information systems have become so pervasive and so complex that users have become a weak link in the security chain. End users of our systems should receive proper security training which includes basic awareness and operational techniques to secure the systems they use. Security polices need to be clear and responsive to the threat involved and users need to know why they are required to use these "extra steps" when they are just trying to get their job done.

The Department has had the challenge of putting together 22 different agencies and components, each with its own security policies and culture. This includes putting together various facilities that have been transferred to DHS oversight such as the Plum Island Animal Disease Center the Department took over from the USDA. No doubt, this is a tough job.

I am happy to have the Department's Chief Information Officer, Mr. Scott Charbo, here to testify how he has faced the challenge of combining the legacy systems into a single system and how he has designed the security program to protect the Department's networks and systems. I imagine GAO will offer some constructive criticism and provide workable recommendations for the Department to work with in the future to better secure its systems.

Beyond the operational responsibilities of Mr. Charbo, there are aspects of the Departments' other cybersecurity programs I would like this subcommittee to investigate. Specifically, I am concerned that the Department's efforts to secure the country's information infrastructure are lacking in organization and coordination with

the private sector and experts in the field. While this is beyond the responsibilities of Mr. Charbo, I am interested to see how the Department has worked with the private sector to map vulnerabilities and implement mitigation efforts to protect the country as a whole. I have said it before, I believe an attack on our information infrastructure could be worse than the effects of a weapon of mass destruction and I would hope the Department takes it just as seriously. I am interested to hear about the coordination role the Department has taken regarding the vulnerabilities facing the Nation's information infrastructure, from secure software development to control system protection measures. I would like to see a report on what the Department has done and a road map for where it plans to go in the future, including what it hopes to accomplish with these future efforts.

Mr. Chairman, I hope this subcommittee can continue to assist the Department in its efforts to protect and secure this Country's critical information infrastructure.

Mr. LANGEVIN. I thank the gentleman.

The Chair now recognizes the Chairman of the full committee, Mr. Thompson of Mississippi, for the purposes of an opening statement.

Mr. THOMPSON. Thank you very much, Mr. Chairman. And good afternoon to our witnesses. I appreciate you for holding this hearing and for your efforts on cybersecurity.

Chairman Langevin touched on the national security implications of this issue, and I would like to associate myself with his remarks. But I would also like to focus my comments this afternoon on a quote by Ralph Waldo Emerson, the great American essayist and poet, who once said, "What you do speaks so loud that I cannot hear what you say."

Two—months ago Assistant Secretary for Cybersecurity Greg Garcia spoke at the Computer Associates World Conference in Las Vegas. There, he told a captive audience several things.

Though security incidents result from exploitation of defects in software design or code, they are also caused by users not fixing their configurations to their security requirements. He also went on to say that security incidents are also caused by insider problems stemming from poor employee training, inconsistent access control policy, and fragmented security implementation and patch management practices.

The Assistant Secretary asked the audience, as he has been asking audiences all over the country, to perform risk assessments on their networks; establish security policies according to risk profiles; invest and upgrade technology solutions, systems, and training; and continue to test, audit, and fix systems.

In light of the materials I have reviewed for this hearing, I think that Mr. Garcia probably should have given that speech to the folk here in Washington, D.C.

Now, there are a lot of folks over in the CIO's office who need to hear that message. How can the Department of Homeland Security be a real advocate for sound cybersecurity practices without following some of its own advice? How can we expect improvements in private infrastructure cyberdefense when DHS bureaucrats aren't fixing their own configurations? How can we ask others to invest in upgraded security technologies when the chief information officer grows the Department's IT security budget at a snail's pace? How can we ask the private sector to better train employees and implement more consistent access controls when DHS allows employees to send classified e-mails over unclassified networks and contractors to attach unapproved laptops to those same networks?

I am not suggesting that the Department discontinue its cybersecurity message to the public and private sectors. But what the Department is doing on its own networks speaks so loud that the message is not getting across to anyone else.

It is not just the private sector that is getting doublespeak from DHS. It is the rest of the Federal Government too. Einstein is the National Cybersecurity Division's sensor system that analyzes suspicious network traffic. Over a dozen Federal agencies use this system. Yet the CIO does not deploy Einstein across the Department. I ask Mr. Charbo today, what kind of message does that send about the Einstein program? If it is good enough for other Federal agencies, why isn't it good enough for DHS?

The "do as I say, not as I do" policy is a recipe for disaster, and if we are serious about the security risks facing our networks, then we need to start acting and stop posturing. I have spent some time reviewing Mr. Charbo's responses to our questions and reviewing the numerous IG and GAO audits of his work. I am not convinced that he is serious about fixing the vulnerabilities in our systems; and if he is not committed to securing our networks, I have to question his ability to lead the Department's IT efforts.

I can't understand for the life of me why it takes outside auditors to tell the CIO and his contractors that these networks are insecure.

The American people are tired of hearing that getting a "D" is a security improvement. I am tired of hearing it.

The American people are tired of hearing their government say one thing but do another.

What happened to leadership? What happened to vision? What happened to accountability? What happened to excellence?

Mr. Langevin, in light of the evidence in front of us today, I think the first thing that Mr. Charbo needs to explain is why he should be able to keep his job.

I thank you for holding this hearing. I look forward to asking the questions of the witnesses, and I yield back the balance of my time.

[The statement of Mr. Thompson follows:]

PREPARED STATEMENT OF OF THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN, COMMITTEE ON HOMELAND SECURITY

I'd like to focus my comments this afternoon on a quote by Ralph Waldo Emerson, the great American essayist and poet who once said: "What you do speaks so loud that I cannot hear what you say.'

Two months ago, assistant Secretary for Cybersecurity Greg Garcia spoke at the Computer Associates World Conference in Law Vegas. There, he told a captive audience several things:

Though security incidents result from the exploitation of defects in software design or code, they are also caused by users not fixing their configurations to their security requirements. security incidents are also caused by insider problems stemming from poor employee training, inconsistent access control policy, and fragmented security implementation and patch management practices.

The Assistant Secretary asked the audience—as he has been asking audiences across this country—to perform risk assessments on their networks; establish security policies according to risk profiles; invest in and upgrade technology solutions, systems, and training; and continue to test, audit, and fix systems.

In light of the materials I've reviewed for this hearing, I think that Mr. Garcia probably should have given that speech to folks here in Washington, D.C.

There are a lot of folks over in the CIO's office who need to hear that message. How can the Department of Homeland Security be a real advocate for sound cybersecurity practices without following some of its own advice? How can we expect im-

provements in private infrastructure cyberdefense when DHS bureaucrats aren't fixing their own configurations? How can we ask others to invest in upgraded security technologies when the Chief Information Officer grows the Department's IT security budget at a snail's pace? How can we ask the private sector to better train employees and implement more consistent access controls when DHS allows employees to send classified emails over unclassified networks and contractors to attach unapproved laptops to the network?

I am not suggesting that the Department discontinue its cybersecurity message to the public and private sectors. But what the Department is doing on its own networks speaks so loud that the message is not getting across to anybody else.

It's not just the private sector that's double-speak from DHS. It's the rest of the Federal government too. 'Einstein' is the National Cybersecurity Division's sensor system that analyzes suspicious network traffic. Over a dozen Federal agencies use this system. yet the CIO does not deploy Einstein across the Department. I ask Mr. Charbo today, what kind of message does that send about the Einstein program? If it's good enough for the other Federal agencies, why isn't it good for DHS?

"Do as I say, not as I do' policy is a recipe for disaster, and if we are serious about the security risks facing our networks, then we need to start acting and stop posturing. I've spent some time reviewing Mr. Charbo's responses to our questions, and reviewing the numerous IG and GAO audits of his work. I am not convinced that he's serious about fixing the vulnerabilities in our systems.

And if he's not committed to securing our networks, I have to question his ability to lead the Department's IT efforts. I can't understand for the life of me why it takes outside auditors to tell the CIO and his contractors that these networks are insecure.

The American people are tired of hearing that getting a 'D' is a security improvement. I'm tired of hearing it.

The American people are tired of hearing there government say one thing but do another.

What happened to leadership: What happened to vision? What happened to accountability? What happened to excellence? In light of all of the evidence in front of us, I think the first thing that Mr. Charbo needs to do is explain to us why he should keep his job.

Mr. LANGEVIN. I thank the chairman.

All the members of the subcommittee are reminded, under the committee rules, opening statements may be submitted for the record.

I now welcome our first panel of witnesses. Our first witness is Scott Charbo, the Chief Information Officer of the Department of Homeland Security. Mr. Charbo leads the resource efforts of the information technology assets supporting 180,000 Federal employees at the 22 agencies now comprising DHS.

Prior to joining DHS in June 2005, Mr. Charbo was the Chief Information Officer at the U.S. Department of Agriculture from August ofμ2002. Mr. Charbo holds a Bachelor of Science degree in biology from the University of Tampa, and a Master of Science degree in plant science from the University of Nevada-Reno.

Our second witness, Gregory Wilshusen, is Director for Information Security Issues at GAO, where he leads information security-related studies and audits of the Federal Government. He has over 26 years of auditing, financial management, and information systems experience. Mr. Wilshusen holds a B.S. degree in business administration, accounting, from the University of Missouri, and an M.S. in information management from George Washington University.

Our third witness is Keith Rhodes, the Chief Technologist of the U.S. General Accounting Office, and Director of the Center for Technology and Engineering. Mr. Rhodes provides assistance throughout the legislative branch on computers and telecommunications issues and leads reviews requiring significant technical ex-

pertise. Mr. Rhodes holds degrees in computer engineering and engineering physics from Ohio State University and the University of California at Los Angeles, respectively. Mr. Rhodes will be supporting Mr. Wilshusen during the question-and-answer period. STATEMENTS OF

STATEMENT OF SCOTT CHARBO, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. LANGEVIN. Without objection, the witnesses' full statements will be inserted into the record. And I now ask each witness to summarize their statement for 5 minutes, beginning with Mr. Charbo.

Mr. CHARBO. Thank you, Mr. Chairman, Ranking Member McCaul, Chairman Thompson, members of the subcommittee, for allowing me this opportunity to testify.

The Department has implemented numerous changes to improve and address emerging information security risks and challenges, while at the same time enhancing information sharing. Key results include the following:

In 2005, the Department baselined the systems inventory, which became the cornerstone for managing the risks and progress within the Department.

In 2006, the plan improved overall security accreditation and certification compliance from 21 percent to 94 percent of the Department's systems.

In 2006 and 2007, the Department has used the DHS inventory and improved security accreditation to help identify the risks to the Department information systems. We have implemented the DHS Security Operations Center and the concept of operations for the SOC. This improved incident handling and reporting process now provides U.S. better situational awareness of our information security posture and improved visibility into component security events.

Since the start of 2007, we have closed 45 percent of the financial system notifications of findings and recommendations, findings on our financial systems within the DHS components.

We have three key initiatives that are taking a more proactive approach to addressing emerging threats in cybersecurity:

The legacy wide area networks, or WANs, are being collapsed into a single WAN called OneNet. OneNet has been designed to enhance security and fully implements the IPSec protocol, ensuring all traffic on the WAN is fully encrypted and authenticated.

The Department is standardizing all electronic mail, e-mail and directory services into a single, secure, modern framework.

The last initiative is to collapse the multiple legacy data centers into a common, shared and secured environment.

This first phase of the consolidation is up and running, and the legacy systems are currently being migrated. As I briefed many of you, a more complete situational awareness picture of our information security posture now ensures that our NOC SOC has better enterprise visibility.

Currently, our data from scans, the DHS SOC, and component reports do not support a position that our networks are compromised or that missions have been impacted. We will continue to diligently monitor and adjust to the changing landscape.

Recently, the GAO completed a review of the information security controls that protect information and security systems used to support the CBP US-VISIT program. The audit lasted for over a year, and many of the findings are based on data from a year ago. The report identified 45 security weaknesses and generated 56 report recommendations. CBP replied to the GAO on June 18th of 2007, with a detailed report, which I will highlight.

The GAO report did not consider compensating or mitigating controls, where legacy or technical barriers make a control impractical to implement. The GAO audit examined the CBP US-VISIT systems without context of the overall CBP environment, including the significant upgrades made over the past year.

For example, password protecting the system BIOS data is a significant technical and operational challenge that is effectively managed through physical security access restrictions and proper user training. Although one control may be deficient at the system level, additional controls exist at the network or facility level to compensate.

Another example, that an Internet service provider had unrestricted direct access to the CBP network was not concurred because the service is staffed by CBP-cleared personnel, with full field background investigations and access limited via a dedicated internal connection for the purpose of network management.

CBP has already taken significant steps towards mitigating many findings that have been verified by the GAO. This is missing from the draft report. The majority of network findings are a direct result of legacy systems still used when CBP did not have the capability of supporting or enforcing many of the newer security controls. They must be secured via compensating controls. These systems are in the process of being replaced.

For example, CBP has completed 50 percent—56 percent of the Microsoft XP Active Directory and Microsoft Exchange upgrades. CBP has upgraded 75 percent of its Novell service from 50 to 6.5, a more secure platform.

Mr. Chairman, my goal as the CIO is to continue the improvements in the Department's security posture by focusing on data, the results, and being proactive. For the remainder of fiscal year 2007, my office will take the following actions:

We are establishing and implementing a configuration board, chaired by the deputy CIO, the highest career IT official in DHS.

The board will review and approve all major configuration changes to the Department's infrastructure that can adversely impact the security posture, as well as review all significant DHS SOC notifications.

We will complete the initial round of compliance reviews for all components that ensure that plans and actions and milestones, POAMs, are being completed, and weaknesses are being retired expeditiously.

We will direct, identify, test, and approve for use standards for removable media devices, focusing on thumb drives that are compliant with FIPS 140–2.

We will complete analysis regarding the mission impact for best methods for monitoring secure socket layer connections.

While many challenges lie ahead, we are committed to bring the right processes, architecture, and resources together to bring a balanced IT security process to the Department.

I thank you for this opportunity, and would be glad to address any questions.

Mr. LANGEVIN. Thank you for your testimony.

[The statement of Mr. Charbo follows:]

PREPARED STATEMENT OF SCOTT CHARBO

Thank you, Mr. Chairman, Ranking Member McCaul and Members of the Subcommittee, for allowing me this opportunity to testify before the subcommittee. My remarks will cover the current status of the Department's information security posture.

You have no doubt heard reports of recent information security incidents at various federal agencies, including the Department of Homeland Security. Certainly, we need to increase our vigilance to ensure that such incidents do not happen again, and, in fact, the recent loss of an external hard drive at the Transportation Security Administration has prompted a comprehensive review of how the Department processes and stores privacy information. My office continues to work closely with the Department's Privacy Office and the Chief Human Capital Office to improve the effectiveness of our controls for privacy information.

The Department takes these incidents very seriously, and will work diligently to ensure they do not recur. I'd like to describe for you some of the significant progress we have recently made in improving information security at the Department. The Department is presently working under a decentralized IT governance model. We have named CIOs and attendant IT support staff in each of the major components comprising the Department. To ensure that this model is effective, Secretary Chertoff recently instituted changes in the oversight functions of the Chief Information Officer for the Department. The revised Management Directive 0007.1 *Information Technology Integration and Management* has increased my authority to manage and direct the Department's information technology programs. Specifically:

1. Components must provide their information technology (IT) budgets annually to the DHS Chief Information Officer for review; I will then make recommendations to the Secretary for final budget submissions to the Office of Management and Budget.
2. Any proposed IT acquisition greater than $2.5 million must be reviewed and approved by the DHS Chief Information Officer. These IT acquisitions are defined as services for IT, software, hardware, communications, and infrastructure.
3. Before IT investment proposals greater than $2.5 million are submitted to the DHS Chief Information Officer for approval, the Department's Enterprise Architecture Board must approve the investment and certify its alignment with the Department's enterprise architecture.
4. I approve the hiring of Component Chief Information Officers, as well as set and approve their performance plans, ratings, and annual award compensation in cooperation with component directors.

The result will be a more coherent and effective utilization of IT resources. IT programs and acquisitions are being reviewed at the Department-level to ensure that they are reconciled with the Department's strategic goals and that information security, enterprise architecture and infrastructure considerations are built into them.

The Department's Information Security Program touches virtually every aspect of IT management, to include budget formulation and implementation, system and network design, enterprise and component specific IT operations, information security policy and architecture, and compliance with the Federal Information Security Management Act (FISMA). My authority over all of these areas directly affects our overall security posture. I would like to mention three key IT consolidation initiatives that we have started to not only better align our shared enterprise environment, but to enhance enterprise information security.

First, we are collapsing multiple legacy wide-area networks (WANs) into a single enterprise WAN, called OneNet. OneNet is based on a comprehensive security architecture that uses the latest IT technologies. For example, the new consolidated WAN fully implements the IPSec protocol, an authentication and encryption protocol that ensures the confidentiality of all data transiting the WAN. And, as a key part of the transition to OneNet, we have also implemented a comprehensive Security Operations Center (SOC) Concept of Operations (CONOP). This CONOP details

more efficient processes for the day-to-day management of security functions for OneNet, as well as for reporting incidents both internally to the SOC, and externally to the United States Computer Emergency Readiness Team (US–CERT) and other Law Enforcement and government agencies when required. To aid this effort, we've created the SOCONLINE Incident Reporting web tool for incident reporting, management and closure.

Second, we are standardizing all email and directory services into a single, modern framework that is much more secure than the legacy environments we inherited. The department had 13 different email systems when it was formed. We have standardized the Target Enterprise Architecture for email, deployed a Global Address List and are on track to transition all components to the new email standards by December of 2007. These improvements will eliminate several security vulnerabilities in our email posture and simplify its management.

Third, we are collapsing multiple datacenters into a common shared environment. The first phase of our first datacenter is up and running in Stennis, Mississippi, and we are now in the process of migrating legacy systems into that center. Security has been designed into the Stennis facility from the start and as systems migrate to that facility our security posture will continue to improve.

These initiatives will not only enhance our ability to store, process, and share information, they will also enhance our ability to ensure the confidentiality, integrity, and availability of that information.

In addition to these three major consolidation activities, I have also begun another activity in conjunction with the Chief Financial Officer to enhance the security of our core financial systems. Each component CIO and CFO jointly presented a detailed remediation plan for improving the security of our core financial systems; this was done with the knowledge of both our Inspector General and independent auditors. These plans were personally approved by me, the Department CFO, and the Under Secretary for Management. In addition to ensuring the implementation of these plans, my office partners with the CFO and his team on other issues. One example of our continuing collaboration is a series of workshops that my office has sponsored to assist components in improving the security of these core financial systems. Due to the combined CIO/CFO efforts, we are now making significant progress in resolving prior financial audit findings.

It is my responsibility to ensure that our IT systems comply with all federal and department policies. I now review each component's IT budget and expenditures as outlined in the Exhibit 53s and 300s and ensure their alignment in the following areas:

1. The Secretary's goals and priorities;
2. The Department's enterprise architecture;
3. Needs definition and business case alignment;
4. Privacy rules and regulations;
5. Section 508 (Accessible Systems and Technology) compliance;
6. Information security compliance; and,
7. IT infrastructure compliance.

In 2007, the Department will spend approximately $4.9 billion for information technology, and $332 Million of that is dedicated to IT security. We have requested $5.2 billion for IT in 2008, and we are planning to spend $342 Million on IT security. These numbers represent approximately 6.8 % of the total IT budgets for each of those years. Last week, I completed reviews for all component-level IT budgets for fiscal years 2009—2013. These detailed reviews provided me valuable insights into all areas of the Department's information technology programs, and it has given visibility into departmental activities in information technology from strategic mission, portfolio, and technology perspectives. These reviews will allow me to make informed recommendations to the Secretary concerning the Department's IT budget for these future years, while ensuring that all program elements, especially IT security, are adequately addressed.

On the expenditure side, we are working to make sure our acquisitions are in line with our requirements for information security; so far, I have conducted 130 IT Acquisition reviews for security compliance (as well as enterprise architecture, infrastructure compatibility, business case maturity, etc.), and I have favorably adjudicated many issues to ensure that information security requirements are met in all IT acquisitions.

As part of the process of reviewing and making recommendations for component IT budgets, I also take into account components' performance in mitigating their information security vulnerabilities. Included in this improved Management Directive is the authority to recommend budget changes in areas where a component's information security posture is weak. While I have not yet recommended that a component's budget be modified in response to a lack of success in mitigating

vulnerabilities, I have provided guidance and direction, both informally and in some cases in writing, to the components that are not satisfactorily progressing in their remediation efforts, and with recommended changes.

To ensure compliance with the Federal Information Security Management Act (FISMA), my Chief Information Security Officer (CISO) maintains a comprehensive systems inventory of all government-owned and contractor-managed systems. The Department's Office of Inspector General has reviewed the inventory methodology and continues to give it high marks for both completeness and accuracy. DHS's Information Security Program has made measurable progress, enough that unlike all previous years the Inspector General's annual FISMA assessment did not rate it as a significant deficiency in 2006.

System owners, government and contractor alike, are held accountable for completing all elements of FISMA compliance for each system. The CISO produces a monthly scorecard, providing each component with an honest assessment of their status. Each component is provided a current assessment on status of certification and accreditation for every system in the inventory, annual controls testing, incident reporting, configuration management, information security training, and information security vulnerability management. The scorecards address the security of internal DHS systems as well as contractor operations. Additionally, the CISO has teams in place that conduct regular training and assist visits, with the current emphasis on vulnerability resolution and configuration management.

I review this scorecard with all component CIOs in regular meetings set aside for this purpose and we discuss the scorecard at Management Council at least monthly. I also present this scorecard to the Secretary and Deputy Secretary periodically, and they in turn emphasize security with agency heads as appropriate. Most of our components have made exceptional progress in improving their overall FISMA posture. Since March 2007, I have written letters to the Directors of three components pointing out program deficiencies and suggesting ways to improve.

While the monthly scorecard is the most visible product of the Department's Information Security Program, there is also a continuing emphasis on the basic tenets of effective information security with the understanding that progress in large federal agencies can only be achieved in increments. The Department's Information Security Program is in the third phase of its 5-year strategic plan.

In the first phase, the Program focused on "establishing a baseline." Basic information security policy and architecture were established and automated tools for enforcing the Department's policy were implemented. A thorough inventory of the Department's IT systems was conducted and system owners were identified to ensure accountability for system security.

In the second phase, the Program focused on completing the accreditation of its IT systems. The significant goal of documenting and accepting system risk was accomplished. The implementation of the *FY 2006 Certification and Accreditation (C&A) Remediation Plan* generated a 68 percent increase in the number of systems accredited. The Department's C&A completion rate went from 26 percent in October 2005 to 95 percent by the end of 2006.

We now have a steady-state baseline from which to build. Our security policies and architecture are continually updated to respond to changing federal guidance, evolving missions, and new threats, and the certification and accreditation process is institutionalized across the Department. The current and future phases of the Information Security Program are aimed at incrementally "raising the bar", and our focus is not only on improving the documentation of controls and processes, but, more importantly on enhancing the operational security of every system.

To this end, we are now evaluating and improving systems security profiles at the system level, and, review teams are providing assistance to Components in improving security plans and contingency plans, as well as providing assistance in other areas including configuration management and vulnerability remediation. We currently have over 4000 IT security related Plans of Action and Milestones (POAM) active, all targeting weaknesses identified through internal systems-level reviews, including certification and accreditation and annual assessments, as well as external audits including those conducted by our Inspector general and the Government Accountability Office. So far in 2007, we have completed remediation efforts for over 7000 weaknesses, and all of the weaknesses identified in the recent GAO Audit of the US-VISIT Program now have active POAMs with scheduled completion dates by the end of 2007. We have also completed several tests starting with our most sensitive systems and our Network Perimeters.

Although we still have a ways to go, we've made measurable improvements in the management of information security at the Department. We're not the only ones making this point. The Office of Management and Budget's (OMB) 2006 Report to Congress noted the significant progress we've made in certifying and accrediting the

Department's IT systems. I am confident that the DHS Information Security Program is moving in the right direction and I look forward to working with you and your staff in the future.

Thank you and I look forward to your questions.

Mr. LANGEVIN. The GAO submitted one testimony for the record, but we have two witnesses on the panel to answer questions from the subcommittee. And at this time, I now recognize Mr. Wilshusen to summarize his statement for 5 minutes. Mr. Wilshusen.

STATEMENT OF GREG WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES

Mr. WILSHUSEN. Chairman Langevin, Ranking Member McCaul, Chairman Thompson, and members of the subcommittee, thank you for inviting me to participate in today's hearing on information security at the Department of Homeland Security, DHS. I am joined by Mr. Keith Rhodes, the GAO's chief technologist.

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies such as DHS, where maintaining the public's trust is essential.

The Homeland Security Act of 2002 created DHS by merging components of 22 Federal agencies and components. Each of these brought with it management challenges, distinct missions, unique IT resources and systems, and its own policies and procedures, thereby making implementation and integration of an effective department-wide information security program a significant challenge. Today, I will discuss the implementation of DHS's security program and the effectiveness of computer security controls for key information systems.

Shortcomings of DHS security programs persist, although some progress has been made. In 2005, we reported that DHS had not fully implemented a comprehensive, department-wide program to properly protect the information systems that support its operations and assets. For example, the Department did not have a complete inventory of its systems, and component agencies did not fully or effectively perform key program activities, such as developing risk assessments, preparing security plans, testing and evaluating the effectiveness of security controls, completing remedial actions from known vulnerabilities, and developing and testing continuity of operations plans. We recommended that DHS take specific actions to address these problems.

Since our 2005 report, DHS has taken steps to improve its security program. For example, it completed an inventory of its major systems for the first time in fiscal year 2006. DHS also implemented key program activities, such as contingency plan testing, security control testing, and system certification and accreditation on an increasing percentage of its systems. However, the quality and effectiveness of these activities was not assured, and program deficiencies continue to exist. These deficiencies contribute, Mr. Chairman, to serious computer security control weaknesses that threaten the confidentiality, integrity, and availability of key DHS systems.

For example, DHS's independent auditors reported that security over its financial systems was a material weakness and internal control for fiscal year 2006.

In addition, GAO determined that key systems operated by one of DHS's components, the U.S. Customs and Border Protection, were riddled with control weaknesses and did not effectively prevent, limit, and detect access to its computer networks systems and information.

For example, it did not adequately identify and authenticate users, sufficiently limit access to information and information systems, properly protect external and internal boundaries of computer networks, effectively implement physical security at several locations, or provide adequate log-in or user accountability for key information technology resources. As a result, increased risk exists that unauthorized individuals, internal and external to the organization, could read, copy, delete, add, and modify sensitive and personally identifiable information and disrupt service on DHS systems.

We are making recommendations to the Department to help it address these issues.

In summary, DHS has made some progress in implementing its department-wide information security program. However, deficiencies in program activities continue to exist and contribute to serious control weaknesses. Until DHS and its components act to fully and effectively implement its security program and mitigate known weaknesses, they will have limited assurance that sensitive information and computer systems will be sufficiently safeguarded or that departmental missions and goals will be achieved.

Mr. Chairman, this concludes my statement. Mr. Rhodes and I would be happy to answer questions.

[The statement of Messrs. Wilshusen and Rhodes follows:]

PREPARED STATEMENT OF GREGORY C. WILSHUSEN

Mr. Chairman and Members of the Committee:

Thank you for inviting us to participate in today's hearing on information security at the Department of Homeland Security (DHS). Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies such as DHS, where the public's trust is essential. For many years, GAO has reported that poor information security is a widespread problem with potentially devastating consequences. In reports to the Congress since 1997,[1] GAO identified information security as a governmentwide high-risk issue.

In this testimony, GAO discusses DHS' department-wide information Security program and computer security controls for key information systems. We based this testimony, in part, on our previously issued reports,[2] and our draft report—that has been provided to DHS for review and comment—on computer security controls for certain information systems operated by the U.S. Customs and Border Protection (CBP). We also considered our analysis of the department's annual Federal Information Security Management Act (FISMA)[3] reports for 2005 and 2006 and the depart-

[1] GAO, *High-Risk Series: An Update,* GAO–07–310 (Washington, D.C.: January 2007).

[2] GAO, *Information Security: Department of Homeland Security Needs to Fully Implement Its Security Program,* GAO–05–700 (Washington, D.C.: June 2005) and *Information Security: Department of Homeland Security Faces Challenges in Fulfilling Statutory Requirements,* GAO–05–567T (Washington, D.C.: April 2005).

[3] FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107–347 (Dec. 17, 2002) and requires agencies and their inspectors general or independent external auditors to report annually on the effectiveness of their security policies and compliance with the requirements of the Act. GAO, *Informaion Security: Agencies Report Progress But Sensitive Data*

ment's performance and accountability report for 2006. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

Shortcomings in DHS information security program although progress has been made. In 2005, we reported that DHS had not fully implemented a comprehensive, department-wide information security program to protect the information and information systems that support its operations and assets. For example, the department did not have a complete inventory of its systems and component agencies did not fully or effectively perform key program activities such as developing risk assessments, preparing security plans, testing and evaluating the effectiveness of security controls, completing remedial action plans, and developing and testing continuity of operations plans. We recommended that DHS take specific actions to address these problems. Since our 2005 report, DHS has taken steps to improve its security program. For the first time, DHS completed a comprehensive inventory of its major applications and systems in fiscal year 2006. DHS has also implemented a department-wide tool that incorporates the guidance required to adequately complete a certification and accreditation for all systems and has implemented key program activities such as contingency plan testing, security control testing, and system certification and accreditation, on an increasing percentage of its systems. However, the quality or effectiveness of these activities was not assured and deficiencies continue to exist.

These program deficiencies contribute to significant weaknesses in computer security controls that threaten the confidentiality, integrity, and availability of key DHS information and information systems. For example, DHS' independent auditors reported that security over its financial systems was a material weakness in internal control for fiscal year 2006. In addition, GAO determined that CBP did not implement controls to effectively prevent, limit, and detect access to certain computer networks, systems, and information since it did not (1) adequately identify and authenticate users; (2) sufficiently limit access to information and information systems; (3) ensure that controls adequately protected external and internal boundaries; (4) effectively implement physical security at several locations; (5) consistently encrypt sensitive data traversing the communication network; and (6) provide adequate logging or user accountability for the mainframe, workstations, or servers.

CBP also did not always ensure that responsibilities for system development and system production were sufficiently segregated. As a result, increased risk exists that unauthorized individuals, internal and external to the organization, could read, copy, delete, add, and modify sensitive and personally identifiable information and disrupt service on DHS systems.

Until DHS and its components act to fully and effectively implement its security program and mitigate known weaknesses, they will have limited assurance that sensitive information and computer systems will be sufficiently safeguarded or that departmental missions and goals will be achieved. Implementation of GAO's recommendations will assist DHS in mitigating the deficiencies described in this statement.

Background

To address the challenge of responding to current and potential threats to homeland security—one of the federal government's most significant challenges—the Homeland Security Act of 2002 mandated the merging of 22 federal agencies and organizations to create the Department of Homeland Security (DHS). Not since the creation of the Department of Defense in 1947 has the federal government undertaken a transformation of this magnitude. Each of the 22 agencies and organizations brought with it management challenges, distinct missions, unique information technology infrastructures and systems, and its own policies and procedures, thereby making the implementation and integration of an effective department-wide information security program a significant challenge.

DHS' mission, in part, is to prevent and deter terrorist attacks within the United States,[4] reduce the vulnerability of the United States to terrorism, and to minimize the damage, and assist in the recovery, from terrorist attacks that do occur.[5] One of the department's components, the United States Customs and Border Protection (CBP), is responsible for securing the nation's borders.

Remains at Risk, GAO–07–935T (Washington, D.C.: January 2007) describes the results of GAO's analysis of the 2006 FISMA reports for 24 agencies including DHS.

[4] 6 U.S.C. § 113(a).

[5] 6 U.S.C. § 111(b).

Virtually all DHS and CBP operations are supported by automated systems and electronic data, and the agency would find it difficult, if not impossible, to carry out its mission and account for its resources without these information assets. Hence, the degree of risk caused by security weaknesses is high. For example, resources (such as payments and collections) could be lost or stolen, data could be modified or destroyed, and computer resources could be used for unauthorized purposes or to launch attacks on other computer systems. Sensitive information could be inappropriately disclosed, browsed, or copied for improper or criminal purposes. Critical operations could be disrupted, such as those supporting homeland security and emergency services. Finally, DHS' missions could be undermined by embarrassing incidents, resulting in diminished confidence in its ability to conduct operations and fulfill its fiduciary responsibilities.

According to FISMA, the Secretary of DHS is responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems used by the agency or by a contractor on behalf of the agency. The Secretary has delegated to the DHS Chief Information Officer (CIO) responsibility for ensuring compliance with federal information security requirements and reporting annually to the Secretary on the effectiveness of the department's information security program. The CIO designated the Chief Information Security Officer (CISO) to

- develop and maintain a department-wide information security program, as required by FISMA;
- develop departmental information security policies and procedures to address the requirements of FISMA;
- provide the direction and guidance necessary to ensure that information security throughout the department is compliant with federal and departmental information security requirements and policies; and
- advise the CIO on the status and issues involving security aspects of the departmentwide information security program.

Shortcomings in DHS Information Security Program Remain Although Progress Has Been Made

In 2005, GAO reported[6] that DHS had not fully or effectively implemented a comprehensive, department-wide information security program to protect the information and information systems that support its operations and assets. Although DHS had developed and documented policies and procedures that could provide a framework for implementing the department's program, certain departmental components had not yet fully implemented key program activities. For example, components' weaknesses in implementing these activities included (1) incomplete risk assessments for determining the required controls and the level of resources that should be expended on them; (2) missing required elements from information system security plans for providing a full understanding of the existing and planned information security requirements; (3) incomplete or nonexistent test and evaluation of security controls for determining the effectiveness of information security policies and procedures; (4) missing required elements from remedial action plans for identifying the resources needed to correct or mitigate identified information security weaknesses; and (5) incomplete, nonexistent, or untested continuity of operations plans for restoring critical systems in the case of unexpected events.

The table below indicates with an "x" where GAO found weaknesses with key information security program activities for six systems and applications reviewed at four components.

The table below indicates with an "x" where GAO found weaknesses with key information security program activities for six systems and applications reviewed at four components.

Table 1: Weaknesses in Information Security Program Activities for Selected Systems

DHS SYSTEM	DHS component	Risk assessment	Security plan	Security test and evaluation	Remedial action plans	Continuity of operations
Major application	US-VISIT	n/a	X[a]	n/a	n/a	n/a

[6] GAO–05–700.

DHS SYSTEM	DHS component	Risk assessment	Security plan	Security test and evaluation	Remedial action plans	Continuity of operations
Major application	ICE			X	X	X
Major application	TSA			X	X	X
General Support system	ICE	X		X		X
General Support system	TSA	X		X	X	X
General Support system	EP&R	X	X		X	X

Source: GAO analysis of information security documentation for United States Visitor and Immigrant Status Indicator Technology (US–VISIT), Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), and Emergency Preparedness and Response (EP&R) systems.

a For each system, we obtained and reviewed all documentation contained in the certification and accreditation package—with the exception of US–VISIT—in this case, we reviewed only the security plan.

We also reported that DHS had not yet fully developed a complete and accurate systems inventory and used an enterprise management tool, known as Trusted Agent FISMA, that contained unreliable data for overseeing the components' reported performance data on their compliance with key information security activities. The DHS Inspector General reported that the data in the tool were not verified, there was no audit trail capability, material weaknesses were not consistently reported or linked to plans of action and milestones, and plans of action and milestones that had been identified and documented were not current.

To assist DHS in addressing these issues, we recommended that it establish milestones for verifying the components' reported performance data in Trusted Agent FISMA and instruct its component agencies to

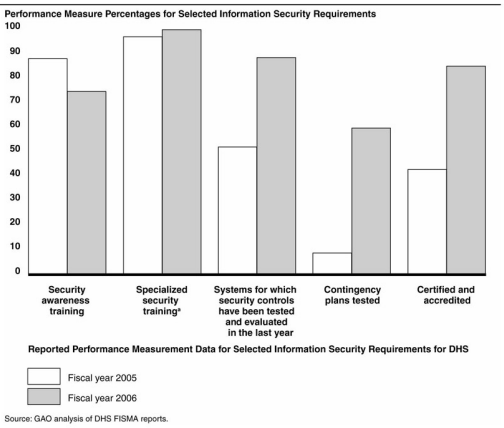
- develop complete risk assessments;
- document comprehensive security plans;
- fully perform testing and evaluation of security controls;
- complete remedial action plans; and
- develop, document, and test continuity of operations plans.

DHS Has Taken Steps to Improve Security Program, but Deficiencies Persist

In response to our recommendations, the department has made several improvements in its information security program. For example, DHS officials stated that they had developed a plan to address all of the recommendations in our 2005 report. For the first time, DHS completed a comprehensive inventory of its major applications and general support systems, including contractor and national security systems, for all organizational components in FY 2006. DHS also implemented a departmentwide tool that incorporated the guidance required to complete a certification and accreditation [7] for all systems. The completion of these two tasks eliminated two factors that had significantly impeded the department in achieving some success in establishing its security program over the previous two years. In addition, the CISO revised the baseline information technology security policies and procedures and mandated that the components ensure that their systems meet the requirements specified in the DHS baseline configuration guides.

With the exception of providing security awareness training to employees, the department has also implemented key program activities such as conducting specialized security training, testing and evaluating controls, testing contingency plans, and certifying and accrediting systems, for an increasing percentage of its systems or personnel in FY 2006 (see figure below).

[7] Certification is the comprehensive evaluation of the management, operational, and technical security controls in an information system to determine the effectiveness of these controls and identify existing vulnerabilities. Accreditation is the official management decision to authorize operation of an information system. This authorization explicitly accepts the risk remaining after the implementation of an agreed-upon set of security controls.



However, the quality or effectiveness of certain information security program activities has not been assured. Although CBP has made important progress in implementing the department's information security program, it has not fully or effectively implemented key program activities. For example,

- Risk assessments performed for systems supporting a key border protection program did not always fully characterize risks to the systems;
- Interconnection security agreements listed in the security plan for a key system were not current;
- Procedures for testing and evaluating the effectiveness of security controls were not sufficient and did not reveal problems with a mainframe computer that potentially allowed unauthorized users to read, copy, change, delete, and modify sensitive information;
- CBP did not always address significant deficiencies in a remedial action plan thereby exposing sensitive information to increased risk of unauthorized disclosure or modification;
- CBP did not adequately establish and implement tools and processes to ensure timely detection and handling of security incidents; and
- CBP had incomplete or out-of-date privacy documents for systems supporting a key border protection program.

Significant Control Weaknesses Place Sensitive Information and Operations at Risk

Significant weaknesses in computer security controls threaten the confidentiality, integrity, and availability of key DHS information and information systems.

Independent external auditors identified over 130 information technology control weaknesses affecting the department's financial systems during the audit of its fiscal year 2006 financial statements. Weaknesses existed in all key general controls and application controls. For example, systems were not certified and accredited in accordance with departmental policy; policies and procedures for incident response were inadequate; background investigations were not properly conducted; and security awareness training did not always comply with departmental requirements. Additionally, users had weak passwords on key servers that process and house DHS financial data, and workstations, servers, and network devices were configured without necessary security patches. Further, changes to sensitive operating system settings were not always documented; individuals were able to perform incompatible duties such as changing, testing, and implementing software; and service continuity

plans were not consistently or adequately tested. As a result, material errors in DHS' financial data may not be detected in a timely manner.

Although CBP has made progress in addressing security vulnerabilities, significant problem areas still remain. Certain CBP systems supporting a key border protection program were riddled with control weaknesses that placed sensitive and personally identifiable information at increased risk of unauthorized disclosure and modification, misuse, and destruction possibly without detection, and placed program operations at increased risk of disruption. Weaknesses existed in all control areas and computing device types reviewed. Deficiencies in controls intended to prevent, limit, and detect access to information and information systems exposed CBP's mainframe computer, network infrastructure, servers, and workstations to insider and external threats, as the following examples demonstrate. CBP did not:

- Adequately identify and authenticate users in systems. For example, passwords were transmitted over the network in clear text and were stored using weak encryption.
- Sufficiently limit access to information and information systems. For example, over one thousand users with command line access could put a program designed to bypass security rules into a special system library.
- Ensure that controls adequately protected external and internal network boundaries. For example, internal network traffic was not segregated. Moreover, workstations and many servers did not have host based firewalls.
- Effectively implement physical security at several locations. For example, CBP did not control access to its restricted information technology spaces since its physical access systems were controlled by local authorities.
- Consistently apply encryption to protect sensitive data traversing the communication network. For example, network routers, switches, and network management servers used unencrypted network protocols so that files traversing the network could be read.
- Adequately provide audit logging or user accountability for the mainframe computer, workstations, or servers. For example, monitoring lists for key operating system libraries did not capture needed data for all sensitive libraries in the desired locations.
- Always ensure that responsibilities for system development and system operations or production were sufficiently segregated. For example, mainframe system programmers were allowed to access application production data and developmental staff could access mainframe operating system libraries. Moreover, developmental staff had update access to the application production data.
- Consistently maintain secure configurations on the mainframe, applications servers, and workstations we reviewed at the data center and ports of entry. For example, production servers and workstations were missing critical operating system and software application security patches.

As a result, increased risk exists that unauthorized individuals, internal and external to the organization could read, delete, add, and modify sensitive and personally identifiable information and disrupt service on DHS systems.

To assist enhance departmental security, GAO has previously made recommendations to DHS in implementing its information security program and is making additional recommendations in two draft reports currently being reviewed by the department. Implementation of these recommendations will facilitate improvements in the department's information security posture.

In summary, DHS has made progress in implementing its departmentwide information security program. However, the effectiveness of its program is not assured. Deficiencies in key program activities continue to exist and contribute to significant computer security control weaknesses that place (1) sensitive information and information systems at increased risk of unauthorized disclosure, use, modification, or destruction, possibly without detection, and (2) agency operations at risk of disruption.

Ensuring that weaknesses are promptly mitigated and that controls are effective will require senior management support and leadership, disciplined processes, and effective coordination between DHS and its components. It also requires consistent oversight from the Secretary of DHS and the Congress. Until DHS and its components act to fully and effectively implement its information security program and mitigate known weaknesses, limited assurance will exist that sensitive information will be sufficiently safeguarded against unauthorized disclosure, modification, and destruction, or that DHS programs will achieve their goals.

Mr. Chairman, this concludes our statement. We would be happy to answer your questions.

VerDate Nov 24 2008 09:38 Aug 12, 2009 Jkt 000000 PO 00000 Frm 00025 Fmt 6633 Sfmt 6621 H:\DOCS\110-HRGS\110-52\48926.TXT HSEC PsN: DIANE

Mr. LANGEVIN. I thank you, Mr. Wilshusen, for your testimony. I thank the panel for their testimony.

I remind each member that each member will have 5 minutes to question the panel, and I now recognize myself for 5 minutes.

Mr. Charbo, what we found in terms of staff investigative work, and also the GAO report, is very disturbing in terms of weaknesses in security at the Department of Homeland Security. I want to begin my questioning by asking this:

Several months ago, hackers operating through Chinese Internet service launched an attack on the computer system at the Bureau of Industry and Security at the Department of Commerce. Hackers operating through Chinese Internet servers also accessed networks at several State Department locations, including its Washington headquarters and inside the Bureau of East Asian and Pacific Affairs.

Now, we are familiar with public reports about the cyberattacks against the Department of Defense that were once code-named Titan Rain. As I mentioned in my opening statement, the infiltration of our data is a serious problem. And I want to know what the Department has done to stop it.

Have you ever requested or received intelligence briefings about Chinese hackers penetrating Federal networks? And on a scale of zero to 10, how concerned are you about this threat?

Mr. CHARBO. Myself, I have not received an intel brief on those incidences. We have had an intel brief that was coordinated through the Federal CIO counsel with OMB through the support of DOD that did not report directly back to any evidence within DHS of any incidences from that data. It did identify other departments, but it did not point back to DHS.

Do we experience scans from foreign countries? We believe so; we report those. Those are not penetrations. From a scale of one to 10, it is significant. It would be at a high scale in terms of a concern.

I believe we do have a decent perimeter for the Department, where we are trapping things that come through, but none of those point back to being an orchestrated attack on the Department.

Mr. LANGEVIN. And the other day we had the chance to go over this in a meeting that we had, but for the record, have you ever requested a briefing on those issues?

Mr. CHARBO. Sir, I have not; on those specific issues I have not requested a briefing. We have asked the intel organizations to come in and do monitoring and reviews, using some of their skills, on our system. We have done numerous cases of those.

Mr. LANGEVIN. Mr. Charbo, DHS incident number 2006–09–30 refers to suspicious beaconing activity, or botnets, on DHS computers. Now this is a common method of attack for sophisticated hackers to enter into networks and send out beacons in order to begin infiltrating data.

Have DHS computers ever, quote-unquote, "phoned home" to Chinese servers?

Mr. CHARBO. I have not had any data that supports that. We have a filing within US–CERT. It is important to understand that the US–CERT incidences that we report, this 800 number, that is not a penetration. Those are events that we report up as a data-

gathering tool for DHS, for the Federal Government, for the US–CERT to communicate out.

Of those incidences, they are categorized. You place those into categories of significance based upon what you believe you are seeing at the time when you file that report. We had 844 of those in 2005 and 2006. It varies from "I lost a laptop" to "a phone I lost"; or it was "something was stolen" to "we find malicious ware that is on a laptop." But we are capturing that as it scanned onto the network. It is very important to understand that.

Of those events which are bots, we have—I have no evidence, I have no data that points back that it was actually phoning back to a Chinese network.

Mr. LANGEVIN. Mr. Charbo, I would also like to discuss DHS incident 2006–09–041, where a password dumping utility and other possibly malicious files were found on two DHS systems. This obviously looks like the work of experienced hackers.

Once hackers are inside the system, they perform what is known in the industry as a "rogue tunnel." This tunnel allows them to access the station through a beacon—through a back door, even when it appears that they have been removed from the system.

Now, performing a rogue tunnel audit would allow you to determine whether the hackers are still within your systems. My question is, if you were concerned about bots on your computers, experts suggest conducting ingress and egress filtering on individual client PCs. Yet you report that DHS does not perform rogue tunnel audits nor does it apply ingress and egress filtering. Why not?

Mr. CHARBO. The question was, do we apply ingress and egress filters on client PCs. We do not do that.

Mr. LANGEVIN. Why?

Mr. CHARBO. We do monitor the edge routers.

Mr. LANGEVIN. Why don't you do that?

Mr. CHARBO. Because we monitor the traffic going outside of our Internet gateway, which is where traffic is leaving the Department. So we look at data as it revolves around that.

If we do find evidence that there may be something suspicious happening, if we track something on the network or something comes in through a USB, which is common, or a laptop is remotely removed from the network, because they are mobile, we have people that are out in fields, they won't receive a patch upgrade.

As it comes back into our environment, that configuration is now off; we will trap things. If it has collected a virus that has come in or patches have come into our configuration controls, that may need to be updated.

So we will trap it at that point within our environment, and then we remove that. We report those up.

Mr. LANGEVIN. What about the rogue tunnel audits? I think these sound particularly dangerous, a rogue tunnel on your system. And obviously it is masked, it is very difficult to detect; why aren't you performing rogue tunnel audits?

Mr. CHARBO. What we do when we identify a password or some type of a malicious ware is, we do a forensic analysis of that. That is our mitigation of identifying whether or not there are further actions that need to be taken or reportings up through US–CERT or to our NOC SOC.

VerDate Nov 24 2008 09:38 Aug 12, 2009 Jkt 000000 PO 00000 Frm 00027 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-52\48926.TXT HSEC PsN: DIANE

Mr. LANGEVIN. The Chair now recognizes the gentleman from Texas for 5 minutes.

Mr. MCCAUL. I thank the chairman.

Imagine agents of a foreign power breaking into the Pentagon or the Department of Homeland Security, going into file cabinets and taking out documents, and they were caught. That would be front page, Washington Post. Yet we know these intrusions are occurring in the Federal networks of Federal agencies.

Some say that September the 11th was a failure of imagination. We had information that al-Qa'ida did want to fly airplanes into buildings and into national landmarks. We just didn't take it seriously. And yet here we are, with the status of cybersecurity the way it is, knowing what the threat potentially could be; and I would argue that this Nation is not taking it seriously.

In order to prevent another devastating attack in the United States, we need to step up to the plate.

You know, I see there are several routes of intrusions—one mischief, another one criminal, one espionage, worst case scenario a terrorist attack to shut down our power grids, to wreak havoc with our financial systems. There are many ways that the terrorists could really wreak havoc in this country. That is what this committee is all about.

I think in order to really be able to evaluate a solution, we need to understand what the risk really is. And that is why I have called upon the Department of Homeland Security, and I hope to work with the chairman in introducing legislation that would call for a national strategic vulnerability assessment on U.S. cybersecurity so that we really know what the risk is and that we know how to deal with that risk.

The private sector needs to be a key piece to that. We have our Federal networks and then we have our critical infrastructures in the private sector. Are they properly protected? Is our Federal Government properly protected?

So my question is, to the panel, maybe more to the GAO, is this something that is necessary for the security of the United States, to conduct a national vulnerability assessment on our U.S. cybersecurity? And in doing so, how would you recommend that we do that?

Mr. RHODES. The risk assessment that you are talking about, risk is a function of threat, vulnerability, and impact. So all three pieces have to be done.

Yes, there has to be a threat assessment, but there also has to be a realization of vulnerability, and there has to be an understanding of impact. No one, certainly not I, certainly not my colleague, Mr. Wilshusen, is going to say secure everything, lock everything down. That is impossible. It is also impossible to have perfect security, but you have to drive toward zero tolerance on key systems.

What you are driving at, Mr. McCaul, is that you have to understand what "key" means. And the first point is, what is the threat against the systems you are trying to protect? And you are absolutely right, it is not just the Federal systems. It is that 97 percent of the critical infrastructure that is in private hands. The power grid is not owned by the Federal Government. The power grid is

in private hands. Same with oil. Same with gas. Same with health care. Same with all of those systems.

Well, they all fit under that hierarchy of "critical infrastructure," and unless and until the government is able to translate to the private sector what the real threat is, the private sector is not going to be able to take it to the boardroom and justify it.

So it is important that there is a threat assessment, but everyone also has to understand, that is one-third of the discussion. There is threat, there is vulnerability, and there is impact.

Mr. MCCAUL. In your report you mentioned centralizing the Department's information security policy, which would go a long ways. I think there is a lot of confusion in the Federal Government as to who is in charge, not only within the Federal Government, but also in the private sector. Of course, we have the Department of Homeland Security, and then we have the NSA and the Department of Defense.

Can you make recommendations on that issue?

Mr. WILSHUSEN. Well, indeed, you know, with FISMA, which is the Federal Information Security Management Act of 2002, it establishes responsibilities for the specific agencies in terms of what their roles and responsibilities are in implementing sufficient safeguards within their agencies to protect this information and information assets.

FISMA also requires that OMB and NIS establish government-wide standards and policies for implementing security across the Federal Government. And so those two organizations have a role in determining what the policies and procedures are that other Federal agencies are required to follow insofar as it relates to non-national security systems.

For national security systems, it is a combination of DOD and the Intelligence Community in coming up with those policies and procedures for government-wide use of those types of systems.

Mr. MCCAUL. Mr. Charbo, do you have any comments on just lines of authority, clear lines of authority, and how we can resolve this? Because there is a lot of confusion, in my view.

Mr. CHARBO. Within the Department of Homeland Security, we have two groups that address cybersecurity. There is the Assistant Secretary for Cybersecurity and Communications, Telecommunications. They are focused on this issue with national policies around protecting cyberspace, critical infrastructure around the cyberthreats.

My focus has been on the systems within the Department. I do not work on policy, but we work on trying to implement the policies that are there within our systems and manage towards more secure space. So if we just—as an example, if we take the recent FBI bot press release, they reported over a million, a million bots within the landscape that they had identified on IP addresses, potentially compromised within the Federal Government or within the U.S. Of that, there were about 181 that were government, dot.gov's. The majority of these were edu's, dot.edu's, educational facilities, and dot.com's. The 181, which included the House, the Senate, the Library of Congress, DHS; we had two IP addresses in that group.

One of those, we had looked at. We believed it was a spoof, which means our IP address was being used as a return address from somebody. The other we aren't sure.

As I said, the data—so we are waiting for that. So the operational roles of trying to implement against policies is where my office falls.

The Assistant Secretary would look into the issues that you are addressing. There is a need.

Mr. MCCAUL. I see my time is up. Thank you.

Mr. LANGEVIN. I thank the gentleman for his questions. The gentleman from Texas would also be glad to know that as a result of our first hearing on cybersecurity, the Chair is in the process of drafting legislation on a national threat assessment of cybersecurity; and I certainly look forward to working with you on that legislation.

Before I recognize the gentleman from Mississippi, I also want to mention it is my intention to go for a second round of questions.

The Chair now recognizes the chairman of the full committee, the gentleman from Mississippi, Mr. Thompson, for the purpose of asking questions for 5 minutes.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Mr. Charbo, are you aware of classified e-mails being sent over unclassified networks?

Mr. CHARBO. Yes, sir. It is termed "spillage."

Mr. THOMPSON. Is that considered proper?

Mr. CHARBO. No, sir.

Mr. THOMPSON. What have you done to correct it?

Mr. CHARBO. We have a procedure in place for those types of spillages. It is very closely aligned with our intelligence organization, our INA group, Intelligence and Analysis.

As we go through our reports that we have gone through for the spillages, those that were considered significant—without exception, those were viewed as where somebody who had access to a secure system had typed an e-mail or made reference to a secured item, sent that item back to somebody else on e-mail on an unclassified system, and that person receiving said, I believe that is a secured breach. So we have a process where we notify that—we cleanse those systems.

That is then a security issue, who they work with, the individual, on the breach. Many actions may happen there. It may be they are—their security clearance is removed. They may be removed from duty. But at that point it becomes a security issue with our security officers.

Mr. THOMPSON. So do you consider these spillages significant?

Mr. CHARBO. They are a significant issue. It is a breach if not addressed. I believe what we are showing is that we are addressing those.

This isn't unique to IT. This occurred even when we had no IT, but there were letters, papers, people wrote books. There are methods of handling and redacting spillages like this that go back quite many years.

Mr. THOMPSON. Mr. Rhodes, do you care to comment on that?

Mr. RHODES. Any cross-authority communication, that is, any communication that breaches classification authority is significant,

and it has to be handled. What has to be put in place is not just personnel. There has to be some control environment, so that people can't move from one network to another freely.

It is not—obviously, there has to be a security function that takes place. It has to be a personnel issue. But having free access from one side to the other is not—is only going to foster the problem.

Mr. THOMPSON. I guess my point is, knowing that you have—these situations exist, could we not provide some controls to prevent it for the most part?

Mr. RHODES. Yes.

Mr. THOMPSON. And I think that is the point I am trying to make.

Mr. Charbo, in these spillage instances, can you provide the committee with how many people have been disciplined in this process?

Mr. CHARBO. I can't at this moment. We can get back.

Our procedure is to refer those to our security office, because it may be a legal or a law enforcement issue at that point, so we have to refer those to our security office. And our intelligence office is involved in that as well.

Mr. THOMPSON. Well, please provide us with what you have done on that.

Are you aware of unapproved laptops being connected to our network?

Mr. CHARBO. Yes, sir.

Mr. THOMPSON. Is that proper?

Mr. CHARBO. No, it is not.

Mr. THOMPSON. What did you do or what have you done to prevent it?

Mr. CHARBO. So the process or the ones that are reported—

Mr. THOMPSON. Go ahead.

Mr. CHARBO. The ones that are reported are where a contractor in our facilities happens to plug a laptop into a port. The alarm will go off.

It is important to remember none of those contractors accessed our network. The alarm will go off. And in the cases that I am familiar with, we have escorted that individual off of the premises. Where we have contractors or it is a company that we have on contract, typically what we also do is follow up with security training recommendations around enforcing our policies.

Mr. THOMPSON. I think part of the issue is whether or not we are providing enough training for the people. But I am a little concerned that a contractor could just walk in and plug up a laptop to a system under any protocol.

Mr. Rhodes, you want to care to respond to that?

Mr. RHODES. I think one of the problems that you are describing, the root cause is that contractor staff are so pervasive.

One of the root causes that we saw to a lot of the problems at the Department of Homeland Security when we were doing our testing is that systems are owned and operated by contract staff; therefore, they have free rein. Yes, an alarm goes off, but the contractor ultimately is running and operating the system at hand, and therefore, the contractor can come and go as the contractor pleases.

Mr. THOMPSON. I beg the indulgence of the Chair.

Mr. Charbo, were you aware of these security shortcomings before GAO brought them to your attention?

Mr. CHARBO. All of these issues that we are discussing specific to the Department of Homeland Security are ones that we report through our Security Operations Center. These are the ones that we provided to your letter as a request of events.

I don't look at every one of those. I am not aware of every one of those. I certainly am aware of every one that impacts the mission. I mean, we have hundreds of these items. What we do—what I do is, we look across these categories, we review what incidences are of significance, we address those. We also take a look at these and determine, how do we need to modify our policies and change processes within the Department?

Mr. THOMPSON. And my question is, why did it take GAO to find the weaknesses rather than your own internal operation?

Mr. CHARBO. Sir, GAO didn't point these incidences out to us.

Mr. THOMPSON. Not incidents. CBP, the incidences dealing with CBP.

Mr. CHARBO. Oh, I am sorry. In terms of the GAO report, some of those were POAMs, or Plan of Actions and Milestones within our reporting processes. Others of these are events that were not picked up in audits by CBP.

We use GAO and IG also. We don't disregard the comments that they make.

I do believe that many of the findings in the GAO audit, since it was done, started over a year ago, many of those corrections have taken place.

As in my statement it was said, there are also mitigating controls. In the cases where these employees are working inside a controlled space, we do background checks on those contractors. They do operate alongside our Federal employees. There is also a contracting officer, a program manager, someone who supervises those employees in that space. So it is important to know that those are secured employees.

Mr. THOMPSON. I yield back.

Thank you, Mr. Chairman. You have been very kind.

Mr. LANGEVIN. I thank the chairman.

The Chair now recognizes the gentleman from North Carolina, Mr. Etheridge, for 5 minutes.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Mr. Charbo, we have been talking about the importance of cybersecurity, and I want to know how important you think it is in the effective operations of DHS's IT resources and how important you think it is to our national security.

We have talked about, the chairman, how many incidents we had in 2005 and 2006, and we know about the situations that happened at Defense and at the Department of State; yet cybersecurity spending has remained flat or has fallen at DHS, even as the budget of IT has risen by over 25 percent in recent years.

The IT security budget was less than 10 percent of DHS's total IT spending in 2006, less than 7 percent in 2007, when cybersecurity experts recommended that spending be approximately 20 percent of the IT budget for security. So my question to you is this:

How do you justify this level of investment in cybersecurity at DHS?

Mr. CHARBO. In terms of the budget for the chief information security officer, it did reduce in 2005 to 2006. That was a reflection of our security strategic plan. In 2004, there was a high incidence of what we call "boarding parties." This was trying to determine what the inventory was.

The budget presented back for outyears, which is now in terms of monitoring the progress for security and also on our Security Operations Center, reflects a flat line. It has been $15µmillion for the chief information security officer. That is for policy and for oversight; it is not for just the for what we have been putting into the Security Operations Center.

Mr. ETHERIDGE. Let me help you with that, because for 2005 to 2007, 10 million. And it is truly flat. 2006 is 15, 2007 it is 15.

Mr. CHARBO. Correct.

Mr. ETHERIDGE. And yet we see the incidents going up. We just heard from GAO the problems we have, and yet we aren't investing in protecting the security—

Mr. CHARBO. From 2005 to 2006, it went down. It went up from 2004 to 2005. That represented our plan, our plan of identifying the inventory. The budget presented represented a reduced cost just for monitoring the program.

As far as the Department goes, it has gone up between 2006, 2007 and 2008, not as a percentage, but in dollars.

When I look at a Gartner study—Gartner is a benchmark in the IT industry—their recommendations are 3 to 8 percent in terms of IT investment, depending upon your maturity as an organization. Typically—

Mr. ETHERIDGE. Well, let me interrupt you.

Mr. CHARBO. Yes.

Mr. ETHERIDGE. We are talking about maturity of the organization. We are talking about an organization that is just getting started, that we are putting investment of America's security in.

Are you telling me that we are a mature organization?

Mr. CHARBO. No, sir.

Mr. ETHERIDGE. You were just quoting the statistics from an organization that said it was a mature organization.

Mr. CHARBO. No, sir, the quote I am using is 3 to 8 percent from Gartner based on your maturity, 8 if you are not a mature organization. This is what the study has presented.

We invested in 2006 at about 8.2 percent. We are invested in 2007 at about 7 percent, 6.8; and we are about that amount in 2008 as well.

As a total dollar amount, it has gone up. The request from 2006 to 2007, our requests went up about $20µmillion. Again, in 2008, it went up about $20µmillion, over a base of $350µmillion total in 2008.

Mr. ETHERIDGE. All right. I don't want to spend all my time on this. It is obvious we are not going to agree.

It is not just the dollars we are spending; it is the results we are going to get, and I am very concerned about the results we are getting.

You stated, when the chairman asked you a question earlier about—that you did not get the classified cyberthreat assessment briefing from the Intelligence Community, describing national and State activities.

My question is, why did you not request these briefings?

Mr. CHARBO. You don't know what you don't know, sir. You know, I did not request the briefing because I was not aware of that event, that there were briefings going on that they were providing.

Mr. ETHERIDGE. Why?

Mr. CHARBO. I can't tell you that.

Mr. ETHERIDGE. It seems to me that is an important part of what we are trying to figure out.

Mr. CHARBO. It is. And as we have briefed the chairman, that is an effort that we would appreciate some help on.

Mr. ETHERIDGE. Isn't that part of leadership?

Mr. CHARBO. It is. That is why we are requesting some support in that area.

The first intel briefing that we had on these issues came from a Federal CIO counsel with OMB. I think that most Federal CIOs are in need of that information, and that is an effort that I think the committee can help with. And we are anxious to support that.

Mr. ETHERIDGE. Mr. Chairman, your indulgence. I want to touch one other area, because I think we are into a serious area here.

In view of the recent upticks in cyberattacks across the government systems that we have been talking about, have you requested that DHS conduct a risk assessment—we have talked about it already—to determine what your overall vulnerability is? And why haven't we done it, I guess is the big question.

Mr. CHARBO. At DHS every system goes through a vulnerability assessment as a part of our FISMA, a part of our certification accreditation.

In terms of our major communication networks, our TS networks, our top secret networks, our security networks, our unclassified networks, we have had additional support come in from intelligence agencies to look for additional vulnerabilities in those. Some of those have been completed, some of those we will continue to do. We have some that are scheduled that will continue.

Mr. ETHERIDGE. Thank you Mr. Chairman. I yield back.

Mr. LANGEVIN. I thank the gentleman for his questions.

The Chair now recognizes the gentlelady from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman.

Obviously, there are many, many issues that we will want to be consistently following up on with the Department from the GAO report. And I appreciate your holding this hearing today, and the participation of all the witnesses. I want to just spend a very brief time exploring the US-VISIT issue.

Mr. WILSHUSEN OR MR. Rhodes, can you give us what you found in terms of US-VISIT in cybersecurity? Can you tell us some details of what you found there?

Mr. RHODES. Ms. Lofgren, let me—I want to be careful of the detail, because obviously I don't want to give the—

Ms. LOFGREN. Don't say anything that you shouldn't say in public.

Mr. RHODES. Right. Right. The security issues are pervasive.

There are three parts to this discussion. One, the security issues are pervasive. As a matter of fact, I realize the statement continues to be made that our audit is a year old.

It is not a year old. It started a year ago; the findings are not a year old. As a matter of fact, we curtailed our assessment of the systems because we just kept getting more and more findings. If we had continued to this day, I would argue that we would still be finding things in the environment.

The problems were pervasive, the problems were systemic. It was not a matter of one system here, one system there, one problem here, one problem there. Problems were across the board.

The second point I would make is that actually a lot of those problems can be fixed. They were functions of bad configuration or systems out of date, which is another reason that I say that the problems are systemic, in that, in a lot of ways, they are zero-cost fixes. They are a matter of reconfiguring the system to meet your requirements.

The third point, I reiterate what I said earlier, the systems are run by contractors.

Ms. LOFGREN. No, I got that.

Mr. RHODES. All right. So those are the three—

Ms. LOFGREN. I wonder, could you, Mr. Charbo—we do have a contractor responsible for US-VISIT security, don't we? Could you get us a copy of that contract so we could take a look at that?

Mr. CHARBO. Yes.

Ms. LOFGREN. I appreciate that. On the—back on the US-VISIT, I will ask this, because if it happened, the perpetrators already know that it happened.

Was the database hacked, do you think, Mr. Rhodes?

Mr. RHODES. Was the database hacked? I did not see controls in place that would prevent it. And I did not see defensive perimeters, or I did not see detection systems in place that would let you know whether it had or had not.

Ms. LOFGREN. I will just close.

This morning there was a hearing on US-VISIT and the exit portion, and I had another meeting to go to when our chairperson, Congresswoman Sanchez, asked Mr. Mocny and Mr. Jacksta about the GAO report and cybersecurity issues relative to US–VISIT. And I understand from staff who were—that they were surprised at the findings, and were unable to comment on them.

So I would just ask that, as part of your exiting here, you make a special outreach to those two individuals on this. This is oriented not towards—I mean, we need to improve this situation, especially since much is riding on this. And perhaps we will get the details in a more appropriate setting from the GAO on the details of the exposure and risk, because this is obviously something that we will want to deal with in an expeditious basis.

And I thank the chairman for recognizing me.

Mr. LANGEVIN. I thank the gentlelady for her questions. As I said, we are going to go for a second round of questions.

Mr. Charbo, Chairman Thompson mentioned the Department's problem of saying one thing and doing another. He mentioned the Department's failure to implement Einstein, the National Cybersecurity Division's sensor system that analyzes suspicious network traffic, even though the US–CERT is trying to get other agencies to sign on.

Now, another failure is auditing. DHS has contracts with two clouds to provide service to the Internet, that's Sprint and MCI. With so much traffic coming in and out, these clouds are keeping good traffic in and bad traffic out. Unfortunately, we see in one of your incident reports one of the carriers misconfigured the firewalls and allowed the firewalls to be bypassed.

Now, despite this security breach, DHS has never audited the Sprint cloud. In fact, you told the committee that Assistant Secretary Garcia's shop, the National Cybersecurity Division, should be the one to audit the cloud. Yet, when the committee staff contacted NCSD, they said that not only have they never seen—never been asked to conduct such an audit, but that this should be handled by the CIO's office.

So my question to you is, whose responsibility is it to audit these clouds and why has it never happened before?

Mr. CHARBO. Sir, the responsibilities to us go out to the H router. Those contractors that we have from that carrier, who were administering those, did misconfigure a router. We caught that. We identified that. We changed that. Those were the same cleared employees that—employees we have on staff.

In terms of auditing the carrier clouds, you know, that is essentially auditing the Internet. I do believe that is a larger policy goal than just a Federal CIO's role at DHS or any Federal department. As we discussed, I do think that is an area that could be addressed or should be addressed on a broader scale than just every CIO in the Federal space trying to audit their carriers. There is a contractual issue in that.

Mr. LANGEVIN. You had a direct breach there. There should have been an audit conducted of the cloud. Isn't that—wouldn't that be your responsibility?

And also, how long was that vulnerability open? Do you know how long that vulnerability existed?

Mr. CHARBO. I would have to get back to you on that.

Mr. LANGEVIN. That is disturbing. That is disturbing.

Mr. Charbo, the DHS runs three local area networks, LANs A, B, and C. When was the last time you updated your network topology diagram with a focus on how the unclassified systems connect with the classified systems?

Mr. CHARBO. I would have to get back to you on that, sir, in order of—the exact date of the update of the topology. We have provided the committee with several diagrams of that topology. I would have to get back to you on any recent changes.

Mr. LANGEVIN. Mr. Wilshusen or Mr. Rhodes, if the network topology is incomplete, how can you be certain that your classified networks aren't touching your unclassified networks? And if hackers have infiltrated LAN A, can they have access to other networks within DHS?

Mr. WILSHUSEN. I would say you probably can't be certain whether or not those two networks interconnect if you don't have a list or know all of the interconnections that affect those networks. So the possibility exists. And so certainly that is a key step.

And, in fact, one of the first steps in developing an inventory of your systems and networks is to identify all the interconnections that exist on those networks. So that certainly is a key point of that.

And I would just like to add one thing: Regarding the previous question, we have reviewed, as part of the request, the cloud, if you will, as part of our review of CMS's communication network. And this is what the Centers for Medicare and Medicaid Services, where we looked at the security over the communication network that was contractor-owned, contractor-operated, and identified a number of vulnerabilities that we were able to report on and make recommendations to CMS. And the benefit of that was that CMS took immediate, aggressive action to start implementing those recommendations.

Mr. LANGEVIN. So you would disagree with Mr. Charbo's statement that auditing that cloud would be like auditing the Internet? You are saying that it could be done and it should have been done?

Mr. WILSHUSEN. I am saying there is some benefit to doing so. And we did that on the incidents with CMS.

Mr. LANGEVIN. Mr. Rhodes, do you have anything to add?

Mr. RHODES. Just to reiterate that we did audit the cloud. Now, we audited the portion of the cloud that was within the scope of the requirement from CMS, but we did audit it. So it can be done.

Mr. LANGEVIN. Thank you.

The Chair now recognizes the gentleman from Texas, the ranking member of the subcommittee, for 5 minutes.

Mr. MCCAUL. Thank you. And I want to follow up on your mention of a national strategic vulnerability assessment. I think in light of the testimony it is clear that we need to go forward with that.

I want to follow up on something my colleague, Mr. Etheridge, brought up, and that is the Titan Rain. We had evidence that the Chinese were hacking into our networks at the Department of Defense, at the Commerce Department, State Department, extensive—hitting nonclassified networks, thank God. But that raises some serious concern in terms of the coordination across all Federal levels.

If Mr. Charbo, who is in charge, as the Chief Information Officer, is not aware of that threat, it highlights the problem that we have that no one is really in charge across all Federal levels when you don't have one person in charge. And the coordination piece becomes very important.

Mr. Charbo, I understand none of these intrusions actually hit the Department of Homeland Security, which is probably presumably why you were not briefed on this issue?

Mr. CHARBO. I believe so.

Mr. MCCAUL. Okay.

Mr. CHARBO. I believe so.

Mr. MCCAUL. Have you been briefed since then?

Mr. CHARBO. Briefed on Titan Rain?

Mr. MCCAUL. Right.

Mr. CHARBO. I don't believe specifically. I believe it was a sanitized brief.

Mr. MCCAUL. Were any of your superiors at higher levels briefed on this?

Mr. CHARBO. I couldn't comment on that.

Mr. MCCAUL. Do you see that as a deficit? It seems to me if this is going on, that there needs to be some sort of coordination across particularly the national security-related agencies that this is happening and in order to better protect our Federal Government from these intrusions.

Mr. CHARBO. I agree. I think from my perspective more in-depth intel briefs would be a benefit so that we can react to the situations. As I said, our data comes from what we report through to the US–CERT. We get information back from the US–CERT. That would be our conduit for a lot of these intel briefs. We adjust our systems accordingly from those briefs.

I am trying to establish a regular intel brief for the CIOs within components of the Department to specifically address that issue.

Mr. MCCAUL. I appreciate the challenge you have in your position. It is an enormous one.

Can the Government Accountability Office tell me, this obviously exposes, in my view, a huge vulnerability not only that a foreign government was hacking into major network systems at the Federal level, but also the lack of communication coordination briefings with the Department of Homeland Security in this case.

Mr. WILSHUSEN. I would like to just add to that in terms of there is an organization called the US–CERT which is responsible for collecting and analyzing threat assessments and incidents that occur throughout the Federal Government, and, of course, the agencies are responsible for providing that information to US–CERT. In fact, GAO, we asked for and received a briefing from US–CERT on some of the incidents that you are referring to, particularly with Titan Rain. And so they had the information, and we were able to get some information about that, which helps us to better assess the threats that are out there when we definitely develop our audit programs.

Mr. MCCAUL. Mr. Rhodes, any comment?

Mr. RHODES. I would just say that, yes, there is difficulty in cross-communication. That is why there is a large effort in information sharing, and that what I would convey is that it seems to me that basic curiosity should be driving everyone about their environments. All you have to do is pick up—it is an unclassified document, it is called Unrestricted War. That tells you who your opponent is and tells you how your opponent is coming after you.

Currently there is information about attacks against Italy. Recently there were attacks against Estonia. Prior to that you can just—it doesn't necessarily need to be a decoder—ring—level, supersecret brief in order to understand what is above the fold on the front page of the Washington Post.

Mr. MCCAUL. Just one last point, Mr. Chairman, and that is to follow up on what you are saying, and in my first question talking about the threat posed by al Qaeda and airplanes and not being taken seriously, we clearly have a threat here with cybersecurity.

Do you believe that we are not taking this issue as serious as we should?

Mr. RHODES. My concern is that I don't think people understand that the virtual and the physical world are intersecting every day and becoming more and more intertwined. If we cannot secure systems that are holding information because we do not understand the value of that information, if we can't do the risk assessment based on threat vulnerability and impact, then when the power grid is completely automated, when the oil and gas is completely automated, we will have a very, very serious problem on our hands, because we do have opponents, and they are dedicated.

Mr. MCCAUL. Thank you, Mr. Rhodes.

Mr. LANGEVIN. The Chair recognizes the Chairman of the full committee Mr. Thompson.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Let me at the outset of my questions say that I am real troubled by a statement Mr. Rhodes said that they basically stopped looking at a program because every time they look, they kept finding weaknesses.

Mr. Charbo, I hope you are as equally troubled, too, about that statement from a security standpoint, that basically you—the GAO stopped looking because I would assume that every time they looked, they found a vulnerability. And the fact that we have a private contractor who we will get to contract who is supposed to, I would assume, prevent these things from happening; have you put this contract on notice that their performance is less than stellar in this particular arena?

Mr. CHARBO. Sir, we just received the draft. CBP just commented to the GAO 2 days ago. So there has not been any contractor placed on notice.

Mr. THOMPSON. Well, then are you prepared to tell the committee that based on what GAO found as vulnerability and weaknesses, that you already knew about those vulnerabilities and weaknesses?

Mr. CHARBO. No, sir, I am not prepared to say I already knew about those vulnerabilities and weaknesses. We will sit down with CBP and go through these, as we typically do, go through these and address the contractor issues.

Mr. THOMPSON. Mr. Wilshusen, is it standard operating procedure for a department to contract out its IT security; and if it is, what is the oversight back to that agency if it is contracted out?

Mr. WILSHUSEN. I believe more and more agencies are indeed contracting out IT services, including IT security for certain aspects of that, to include network monitoring and actually administering systems. But it is incumbent upon the agency, and it is required under law that the agency take appropriate oversight measures to ensure that the contractor is applying the appropriate security safeguards and adhering to the agency's own information security policies and procedures.

Under FISMA, the agency is responsible for assuring that the contractor is adequately securing the systems and information that it operates on behalf of the agency.

Mr. THOMPSON. Mr. Charbo, have you certified FISMA compliance with respect to this contract?

Mr. CHARBO. I don't certify FISMA compliance. According to FISMA, the business owner of the system certifies that system.

Mr. THOMPSON. To who?

Mr. CHARBO. Certifies it to the Department, essentially to me. We monitor that, go through and audit those.

Mr. THOMPSON. Can you provide this committee with those certifications?

Mr. CHARBO. I can provide that.

Mr. THOMAS. Well, as whether or not you accepted the certifications?

Mr. CHARBO. Correct.

Mr. THOMPSON. Yield back.

Mr. LANGEVIN. Thank the gentleman.

The Chair now recognizes the gentleman from North Carolina Mr. Etheridge for 5 minutes.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Mr. Charbo, earlier my colleague who had to leave, Ms. Lofgren, was asking GAO some questions as it related to Homeland Security's database, so let me give you a chance to comment, because the question dealt with US–VISIT and the Department's security database, whether or not terrorists or nation states could get into that and change or alter their names and allow them access to this country. And we wouldn't even know that they were doing it, rendering our watch list or our visa tracking protocol useless. When time ran out, you didn't have a response. Did you have a response to GAO's findings on that report?

Mr. CHARBO. The GAO report addresses a CBP system. As we stated in our testimony, there are other controls placed around that system, and there is no evidence that any of those incidents you stated have occurred on that system.

Mr. ETHERIDGE. So you are saying that the US–VISIT database, to your knowledge, has not been hacked by outsiders?

Mr. CHARBO. Correct.

Mr. ETHERIDGE. Let me return to my friend from GAO. Did any of your—Mr. Rhodes—any of the information from the GAO's study indicate any intrusion in the US–VISIT by any outsider?

Mr. RHODES. We did not have any direct evidence of intrusion; however, we did not see controls in place that could prevent it, and we did not see detection systems in place in key areas that would have detected it had there been intrusions.

Mr. ETHERIDGE. So let me reframe my question then. What you are saying is that if someone were smart enough to get in, they could conceivably get in, get out, and never know they had been in.

Mr. RHODES. They might have, sir.

Mr. ETHERIDGE. Let me ask you another question. You mentioned earlier that a low-cost fix to some of the security problems that you found in the US–VISIT system could be done.

Mr. RHODES. Yes, sir.

Mr. ETHERIDGE. How quickly could they be done, and how long would—how long would it take to get them done, and how complicated is it to do them?

Mr. RHODES. The complicated part is figuring out the value of the system and how much security has to be in place. That is a policy analysis. I can't give you that. Once that is established, how-

ever, some of these fixes could be done in an extremely short period of time, a matter of days. This is not weeks or months or years to try and fix things.

When I talk about low cost and reconfiguring a system, I am talking about the time it takes for someone to come in and put a new computer on your desk in your office.

Mr. ETHERIDGE. Mr. Charbo, let me go back to my original question again, because it seems to me, if I am understanding what I am hearing—so if I am incorrect in what I am picking up, please correct me, because I don't know a great deal about it, but I do know this is a very vulnerable area potentially. Is there a reason why we haven't done this?

Mr. CHARBO. As an example of one of the controls that—in the U.S. GAO report on CBP and VISIT is that there is no encryption on the local area network. However, we encrypted the traffic going outside of that network, so there is an encryption control as a mitigating control, plus we do background checks on those employees and contractors that are in that area.

And all of these cases in establishing risk, you look at mitigating controls. If there are some quick, easy configuration control fixes to put in place, we would like to sit down with GAO and understand what those are to implement those.

Mr. ETHERIDGE. Would you mind doing that before you leave today, start that process?

Mr. CHARBO. We have their findings; we have sat down with them.

Mr. ETHERIDGE. Have you already done that?

Mr. CHARBO. I have not. CBP has, US–VISIT has. Their security people have sat down and reviewed the findings, et cetera.

Mr. ETHERIDGE. I would encourage that, because it seems to me that that is a good starting point. Whoever is in charge ought to be knowing what is happening, if I might suggest that.

Mr. RHODES. Mr. Etheridge, may I just add one?

Mr. ETHERIDGE. Please.

Mr. RHODES. Some of these fixes have been made in the time since we made them.

Mr. ETHERIDGE. Thank you.

Mr. RHODES. Some were severe enough that we wanted them fixed right then. But some of them we are in the process of negotiation, because as Mr. Charbo says, he has had the report only a short time.

Mr. ETHERIDGE. In light of that, Mr. Chairman, could we ask that—because I think this is a very critical area, it is a highly vulnerable area—that, Mr. Charbo, if you would please let this committee know as this moves and when these are fixed?

Mr. CHARBO. Yes, sir.

Mr. LANGEVIN. I thank you.

Mr. ETHERIDGE. Mr. Chairman, I yield back.

Mr. LANGEVIN. I thank the gentlemen.

We can clearly go on all afternoon with questions. I am going to ask one final one, and there are several that the committee will have for the panel in follow-up, and we would ask that you get back to us as quickly as possible in writing.

Mr. LANGEVIN. Mr. Charbo, one of your goals that you provide to the committee is 100 percent FISMA compliance, yet we have heard time and again that FISMA compliance doesn't equal security. Many IT security commentators have said that you can't correlate between the grade an agency receives and the true level of security within that agency.

How important is getting an A to you on the FISMA scores, and why isn't your primary focus on securing your own networks and mitigating the vulnerabilities that exist within the networks?

Mr. CHARBO. Sir, FISMA is a law that we are obligated to follow. I mean, if you want to make it a paper process, certainly I believe an organization can make it just a paper process. That is not the case at DHS. FISMA does not require us to stand up a security operations center, as we have reported to the committee with all the actions that happen within the Department. That was an initiative that the Department took, that the CIO's office took, or Chief Information Security Officer took.

So that is where we really believe we are trying to bridge and make FISMA operational. Certainly I do believe it can be just a paper process, but that is not the case at DHS. Our plan of action is in milestones and are very critical in terms of understanding the configuration controls. A lot of the questions have been directed today at how we are going to mitigate those and turn those into operations.

Mr. LANGEVIN. With respect to those POAMs that you have raised, there are a significant number of those POAMs that have not yet been completed and not been addressed. Why is that it. Why is the number so high in terms of POAMs that are unresolved?

Mr. CHARBO. There is a high number, but there have been a high number that have been resolved. The nature of those POAMs is to continuously review the risks, the security postures of your systems, and make a plan of action to mitigate that weakness. There will always be POAMs in the Department if we are doing this correctly and not making it just a paper trail.

Mr. LANGEVIN. Just to quantify, there are, according to the report, 69 percent of the 3,566 open vulnerabilities that exist on the Department's networks, and they did not include the resource to require for mitigating those vulnerabilities. That is a significant number that is still unaddressed, and I hope you are going to get to it.

Mr. CHARBO. In most of those cases, we address mitigating controls.

Mr. LANGEVIN. I want to thank the panel for their testimony today. Again, several times during the hearing you stated that you will get back to us with questions that we had. We will hold you to that. And we ask that you respond as expeditiously as possible in writing to further questions that the committee will have for you.

I want to thank the panel for their testimony today. It has been very valuable. Thank the Members for their questions, and hearing no further business, this subcommittee now stands adjourned.

[Whereupon, at 3:50 p.m., the subcommittee was adjourned.]

VerDate Nov 24 2008 09:38 Aug 12, 2009 Jkt 000000 PO 00000 Frm 00042 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-52\48926.TXT HSEC PsN: DIANE

APPENDIX: Additional Questions and Responses

QUESTIONS FROM HON. BENNIE G. THOMPSON

RESPONSES FROM SCOTT CHARBO

It is my pleasure to provide the following responses to your committee's May 31, 2007 follow-on request for information concerning the Department of Homeland Security's (DHS) information technology security policies and procedures (Attachment 1).[1*]

Question 1.: The network topology diagram provided to the Committee is Incomplete. Please provide the full network topology diagram.

Response: Please find the attached Department of Homeland Security (DHS) OneNet topology diagram. The diagram represents the Department's current infrastructure and details OneNet, DCN, and the Component Connectivity (Attachment 2).[1*] A second diagram shows the Department's A LAN (Attachment 3).[1*] Additional topology diagrams will be provided to your office by Tuesday, June 19, 2007.

Question 2.: Has the Department identified any security Concerns as it moves forward with the proposal, and, if so, what plans are in place to remedy any vulnerabilities prior to convergence of any networks.

The OneNet project is currently managed by the DHS Infrastructure Transformation Program (ITP) within the Office of the Chief Information Officer (DHS CIO). Infrastructure Operations, also an office within the DHS CIO organization, is responsible for the ITP, and provides ongoing assurance that security controls are duly executed in with Chief Information Security Officer (CISO) policies acts as the OneNet Designated Accrediting Authority (DAA).

The OneNet Certification and Accreditation was completed during the implementation stage and achieved anacceptable risk posture in January 2007. An Authority to Operate (ATO) was subsequently issued and residual vulnerabilities, discovered during the accreditation security testing and evaluation (ST&E) process, were entered into the system's Plan of Actions and Milestones (POAM), provided as Attachment 4.[1*] POAM items are being addresesed in accordance with DHS 4300A Attachment H, *Plans of Actions and Milestones process Guide, provided as Attachment 5.*[1*]

The following program issue is being addressed by the DHS CIO in partnership with the DHS service provider, U.S. Customs and Border Protection (CBP).

During the accreditation security testing and evaluation process, we assessed that the security control for audit collection, retention, review, and management was not in place. Customs and Border Protection, responsible through the ITP Charter for One Service Delivery, is fully aware of the audit deficiencies and has a high level security project plan to correct them. The lack of audit management does not pose a risk to the Component Agencies, neither currently nor when they have complete network convergence. Nonetheless, successfully addressing this issue provide the Department with indicators as a security assurance measure that the network has the appropriate security and operational administrative control procedures in place.

Questions 3.: Please provide a list of all mitigation actions tracked within the Department's Trusted Agent FISMA(TAF) tool, including the name of the component, date of assignment, scheduled completion date, mitigation action, and completion date.

Response: A Department-wide is provided in Attachment 4.

Question 4.: Please provide a list of all vulnerabilities that are recorded and tracked within the TAF Plan of Action and Milestone folder, including the name of the component, date of assignment, scheduled completion date, mitigation action, and completion date.

Response: A Department-wide is provided in Attachment 4.

Question 5.: During a meeting with the Committee staff, you stated that you are authorized to reduce funding to agency components that do not mitigate their vulnerabilities in a timely fashion. Please provide a list of funding reductions or recommendations for funding reductions that you made to Secretary Chertoff. Please also provide a narrative of Secretary response to your recommendations.

Response: During the meeting with the Committee staff, the response to the question of the Chief Officer's authority and how he can influence a component's progress was answered in three parts by the Chief Information Officer. To clarify, the Chief Information Officer can make recommendations to the Secretary for budget reductions, but he cannot reduce budgets himself. This three part answer was based on the Secretary's changes to Management Directive 0007.1, *Information Technology Integration and Management.* Additional information follows:

Secretary Chertoff recently instituted changes in the oversight of the Chief Information Officer for the Department of Homeland Security DHS published a revised Management Directive 0007.1 in March 2007, improving the ability of the Chief Information Officer to manage and influence the Department's information technology programs. Included in these changes were:

1. Components must provide their information technology (IT) budgets annually to the DHS Chief Information Officer for review; I will then make recommendations to the Secretary for final budget submissions to the Office of Management and Budget.
2. Any proposed IT acquisition greater than $2.5 million must be reviewed and approved by the DHS Chief Information Officer. IT acquisitions are defined as services for IT, software, hardware, communications, and infrastructure.
3. Before IT investment proposals greater than $2.5 million are submitted to the DHS Chief Information Officer for approval, the Department's Enterprise Architecture Board must approve the investment and certify its alignment with the Department's enterprise architecture.
4. The DHS Chief Information Officer will approve the hiring of Component Chief Information Officers, as well as set and approve their performance plans, ratings, and annual award compensation.

As part of the process of reviewing and making recommendations for component IT budgets, I also take into account components' performance in mitigating their POAM vulnerabilities.

Included in this improved Management Directive is the inherent ability to influence the budget in areas where a component's information security posture is weak. While I have never recommended that a component's budget be reduced due to a lack of success in a I POAM, I have been able to provide guidance and direction to the components that are not satisfactorily progressing in their POAMs. Since March 2007, when the Management Directive gave these additional powers to the Chief Information Officer, I have written letters to the directors of three components pointing out ways they could improve their FISMA scores (See these letters in Attachment 6).[1]*

Indeed, it is not always the best policy to reduce an IT budget if a is not being satisfactorily met. My experience has shown that the components are in fact making efforts to resolve their problems and that the lack of financial means to mitigate vulnerabilities is their primary obstacle to success. We would want to provide encouragement and support to components so that they can obtain additional resources to ensure success.

Question 6.: If you have not provided funding cut recommendations to the Secretary, please provide a list of any components that have not mitigated their POA&M vulnerabilities and a narrative explaining your decision not to recommend a funding reduction.

Response: A Department-wide is provided in 4.

Please see the answer to question 5.

Question 7.: According to the Department's policy on Contractors and Outsourced Operations, "components shall conduct reviews to ensure that the IT security requirements in the contract are implemented and enforced." When was the last Department-wide review of these contracts? Were these reviews conducted by component CIOs or by personnel within your of authority? What vulnerabilities were in the review and when were they remediated? Please provide the Committee with each component review of their outsourced operations, as well as the Departmental review of the components' work.

Response: The Department has a of 717 systems in its inventory. This includes 501 government systems and 216 contractor systems. The Department mandates the

testing of information systems security controls for all systems, government contractor alike, using the National Institute of Standards and Technology (NIST) Special Publication 800–53 (SP 800–53) methodology. Please refer to Attachment 7,[1]* summary of NIST SP–800–53 assessment for a summary of these assessments. Contracting officers and their technical representatives (COTRs) also review contractor performance, including compliance with information security requirements.

Additionally, the Department ensures that IT security requirements are included and enforced in all contracts. To that end, the DHS CIO implemented the IT Acquisition Review (ITAR) process that provides for the DHS CIIO's review of all IT acquisitions of $2.5M or more. Public Law 109–295 requires that "no funds be made available for obligation for any information technology procurement of $2.5M or more without approval of the DHS CIO."

In support of this effort, the CISO developed review criteria and evaluates every Purchase Request (PR) to ensure that the appropriate personnel and information security requirements are included prior to CIO approval and release. The CISO staff has conducted conducted and adjudicated more than 130 PR reviews since October 1,2006. Please refer to Attachment 8,[1]* Summary of Information Technology Acquisition Reviews for a summary of these reviews.

DHS Management Directive 0007.1 requires the DHS CIO to "review and approve all Component IT budgets." The CISO staff completed secwity reviews for more than 375 investments (levels 1 through 4) in April 2007 and provided the security scores to the Capital Planning and Investment Control (CPIC) in support of this requirement. A summary of the results is presented in Attachment 9,[1]* Contractor Monitoring Summary.

Question 8.: According to the Department's policy on Risk Management, "components conduct risk assessments whenever significant changes to the system configuration or to the operational/threat environment have been made, or every three years, whichever comes first." Please provide these risk assessments, including the dates the assessments were conducted.

A complete set of risk assessments is provided in Attachment 10.[1]* Please be aware that this information is considered highly sensitive and should not be released.

Question 9.: According to the Department's policy on IT Security Review and Assistance, "the DHS CISO shall conduct IT security review and assistance visits throughout the Department to determine the extent to which the Component security programs comply with IT security policy, standards, and procedures." When were these security reviews completed? How many components passed or failed this review?

The Department conducts security review and assist visits on an ongoing basis. The Office of Information Security (OIS) IT Security Compliance Team reviews and assesses Certification and Accreditation (C&A), including compliance with the Federal Information Systems Management Act (FISMA).

Documents are reviewed on a pass/fail basis against criteria described in the FY07 Information Security Performance provided as Attachment 11,[1]* the Compliance Team provides Components with feedback on how to raise the quality of systems security, if required.

Plans of Action and Milestones (POAMs) are reviewed monthly and assessed for compliance with OMB guidance and against criteria described in the FY07 Plan. All systems are graded on a pass/fail basis and the Compliance Team tracks Accounting Office (GAO), Office of the Inspector General (OIG) and financial audit findings to ensure that appropriate POAMs have been developed for each recommendation. It also monitors POAMs through completion.

The overall FISMA compliance status for each Component and results of compliance reviews are compiled in a monthly scorecard and distributed to Department ISSMs and CIOs.

Training and assistance provide tailored support designed to help individual Components address compliance issues. In most cases, this involves working directly with Component System Security Managers and Officers (ISSMs and ISSOs) in order to address weaknesses. Security training and assistance visits for FY07 have included:

Training Activities

- C&A
- Risk Management System (RMS) and FISMA (TAF)
- POAM
- Security Awareness
- Role Based Training—Financial System Workshop

Face-to-face and hands-on assistance to help Components understand requirements and conduct activities to ensure improved compliance in the following areas
- C&A
- TAF
- poam
- Financial Audit Remediation Activities

Details for all the activities are provided in Attachment 12.[1]*

Question 10.: The Department's policy on "Wireless Systems" requires "annual security assessments shall be conducted on all approved wireless systems. Wireless security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions." Please provide the Committee with those assessments.

Assessments of the wireless or wired infrastructure are to be completed every three years per Section 3.8.b of DHS Sensitive Systems Policy 4300A version 5.1. The exception to this rule occurs when there is a major configuration change to a system, which requires an immediate re-assessment. Security assessment responsibility is a Component-level activity performed by the Component CIO organizations as part of the DHS security management program.

The Department's Security Certification and Accreditation process, in accordance DHS and NIST security policies and standards, includes the wireless environment when necessitated by mission need in the System Security Life Cycle for each given General Support System. Security assessments for operational wireless systems have been included, as applicable, in the full Security Risk Assessments provided to the Committee in response to Question 8 of your Memorandum.

The DHS Enterprise Architecture recognizes the pervasive need and use of Wireless Systems and has established a Wireless Security Board in collaboration with the DHS Chief Information Security Officer for promulgating wireless policy, standards and assessments for the wireless environment.

Question 11.: When did the Department last audit the MCI MPLS Cloud or the Sprint MPLS Cloud? What were the results of the audit? Did the Department require MCI or Sprint to mitigate vulnerabilities?

The Department has reviewed the security and network operational environments for the two OneNet provided carriers. In 2006, the Department reviewed the carrier services at Sprint during a visit with network steward. The review focused on management and operational issues. However, the review did not cover a technical assessment (security test and evaluation) because the General Services Administration (GSA) is responsible for technical assessments and security validation under both FTS–2001 and Networx. The security inherent in the Dynamic Multiple Virtual Private Network suite of protocols fully protects the confindentiality and integrity of all information transiting the OneNet. The Department has Service Level Agreements with each carrier, attesting that they have established and will maintain conformance with the applicable DHS security controls and availability metrics, which reduces my potential attack on network availability. GSA serves as the government-wide Contracting Officer for the FTS–2001 contract and the upcoming Networx contract is for technical assessments and security validation of the environment. GSA has agreed, during the Networx requirements gathering process, to assume the responsibility for ensuring that the carriers meet or exceed the applicable security requirements of the National Institute of Standards and Technology once the final contract is awarded.

Question 12.: The Committee requested and received a list of FY 2005 and FY 2006 incidents reported to the Department's Security Operations Center (DHS SOC).

a. Please define a "classified data spill." How is this incident different from an incident where a Department employee sends a classified through a non-classified system?

A classified data spill, also referred to as a "classified information or a "collateral information spill," occurs whenever classified information is brought onto a network not approved for the level of classification commensurate with the sensitivity of the information. This can happen through a variety of vectors, including email, Compact Discs, removable media or manual data entry. The Department goes to great lengths to prevent direct electronic transfer between networks, however, when a classified spill occurs, it is usually the result of personnel not following proper classified data handling procedures. A Department employee sending classified information via through a non-classified system is a type of classified data spill.

Under current policy, when a Component or Component Security Operations Center (SOC) becomes aware of a suspected or spillage, it is reported to the DHS SOC either in person or via telephone without delay. Other methods of reporting (Fax, email, DHS SOC Online) me not allowed for this type of incident because they provide additional electronic hails that must also be sanitized, thereby increasing the risk that the information will become accessible to unauthorized persons. Once notified, the DHS SOC coordinates the appropriate required actions.

b. Please explain what disciplinary actions were taken against the contractors in DHS Incident Incident #2006–08–031

Incident 2006–08–031 was entered as a minor incident whereby unauthorized users had attached personal computers to the government network. No access was obtained, and the incident was closed with the following additional action: "Laptops were removed, personnel were escorted off of the premises and training was issued to those who allowed them access to the area.

The full incident report is provided in Attachment 13.[1]*

c. Please provide a list of the FY 2007 incidents reported to the DHS

A list of incidents from October 1,2006 to June 4, 2007 is provided in Attachment 14.[1]*

QUESTIONS FROM THE COMMITTEE ON HOMELAND SECURITY

RESPONSES FROM SCOTT CHARBO

Question 1.: What responsibility does the Chief Information Officer have over networks of the Department of Homeland Security? Please explain your relationship to the Chief Information Security Officer, as well as the Chief Information Officers and Chief Information Security Officers of the Department's component agencies.

Response: The Department's Chief Information Officer exercises all statutory authorities and Federal mandates assigned to Federal Chief Information Officers, particularly those outlined in the Clinger-Cohen Act of 1996 and the Federal Information Security Management Act of 2002 (FISMA). In accordance with FISMA, the Chief Information Security Officer (CISO) is a report to the Chief Information Officer.

Department of Homeland Security Management Directive 007.1, *Information Technology Integration and Management,* included as Attachment 2, further strengthens the role of the DHS Chief Information Officer in three key areas:

- Review and approval authority over all information technology (IT) purchase requests greater than $2.5 million
- Approval over all Component Chief Information Officer
- Input into Component-level Chief Information Officer performance plans and evaluations.

Component Security Programs are under the direction of Component-level Information Systems Security Managers (ISSMs), who report directly to each of their respective Component Chief Information Officers. ISSMs are required to follow guidance the Department CISO. Additionally, ISSMs collectively comprise the Information Systems Security Board (ISSB), which is chaired by the Department CISO.

Question 2.: Please provide the Department's information security policy and incident response plan.

Response: *DHS Sensitive Systems Policy Directive 4300A, Version 5.1 and Attachment F—Incident Response and Reporting* are included as Attachments 3 and 4. These documents represent the Department's current information technology security policy and incident response plan.

Question 3.: Please provide a report on how many and what types of incidents have been reported to US–CERT by agencies within the department of homeland Security. Please categorize each incident using the "Federal Agency Incident and Event Categories" developed by the US–CERT. Please provide details of the attacks during 2004—2007 that were the most critical (classified "CAT 1" on the US–CERT reporting guidelines). Please include both those that were and were not reported to US–CERT, and indicate which were not reported to US–CERT within the US–CERT reporting timeframe.

Individual DHS Components do not report incidents directly to the US–CERT. The Department has its own 24x7 Security Operations Center (DHS SOC) that oversees all IT security operations for the Department. The DHS SOC has direct operational oversight over of all aspects of the Department's common wide area network (OneNet), and also oversees the vulnerability management and incident reporting

processes. Individual Components have security operations capabilities for their own local environments; however, all of these are operationally subordinate to the DHS SOC.

The DHS SOC, and only the DHS SOC, reports incidents to the US–CERT in accordance with US–CERT categorizations and guidelines and in the same manner as the other civilian Federal agencies. Attachment 5 contains a summary report for all incidents reported by the DHS SOC to the US–CERT from October 2004 to the present. The *DHS SOC Security Operations Concept of Operations (CONOPS)* is provided as Attachment 6.

Question 4.: Has the Department taken an inventory of each access point to its network (i.e. every connected device, wireless device, remote device, etc.), both inside and outside of the firewall, in order to identify potential points of vulnerability? Does a complete network topology diagram exist? If so, please provide that diagram.

Response: The network topology diagrams are provided as Attachments 7a and 7b.

Question 5.: Has the Department ever conducted both internal and external penetration tests on its systems? Have individual Components of the Department ever performed internal and external penetration tests on their systems? Please provide copies of all penetration testing reports and narratives describing the vulnerabilities that were revealed and how those vulnerabilities were mitigated.

Response: Current DHS Policy requires all Components to conduct annual vulnerability assessments testing to identify security vulnerabilities on IT systems containing sensitive information. Assessments are also required whenever significant system changes are made. The DHS Computer Incident Response Center (CSIRC), an element of the DHS Security Operations Center (SOC), centrally manages the program, which is executed at the Component level. The CSIRC's role is fully outlined in the SOC CONOPS document (Attachment 5) and is supported within *DHS Sensitive Systems Policy Directive 4300A*[1]* *(Attachment 2).*

DHS Components have implemented internal and external penetration testing programs and currently test all FIPS 199 "high" category systems. General support systems or major applications created or built to meet unique mission needs, receive a full internal penetration test prior to obtaining "Authority to Operate" (ATO). In addition, the DHS Office of the Inspector General (OIG) conducts annual FISMA audits, which include internal penetration testing. Some systems receive periodic manual and automated internal penetration testing. Security Test and Evaluation (ST&E) results, Security Assessment Reports also reveal vulnerabilities. Mitigation actions are uploaded and tracked within the DHS Trusted Agent FISMA (TAF) tool.

Vulnerabilities that can not be mitigated quickly are recorded and tracked within the TAF Plan of Action and Milestone (POA&M) folder. Each item is assigned a scheduled completion date, lists the vulnerability, and articulates how it will be corrected or mitigated.

Attachment 8 provides a representative sample of the Department's penetration testing activities. The aggregate of additional information would reach a National Security classification level. Should you require additional information, please advise and the Department will arrange for courier delivery of information at the appropriate classification.

Question 6.: When was the last time the Department used ingress and egress on client personal computers? When was the last time the Department replicated client-side attacks on those computers? Has the Department ever conducted a network-wide rogue tunnel audit of all client personal computers? Have you ever conducted audits on the aforementioned compromised personal computers from question 3?

Response: DHS does not currently apply ingress and egress filtering on individual client personal computers, however all DHS content to and from the Internet is controlled through dedicated gateways and ingress and egress filtering is enforced at those control points.

The DHS approach is similar to that employed by the Department of Defense (DoD) on its Non-classified Internet Protocol Router Network (NIPRNet) where most of the ingress/egress filtering is done at Internet/NIPRNet gateways. The DoD is conducting a pilot program whereby enterprise-wide client side ingress and egress filtering is currently being tested. DHS will review the results from the pilot and determine the best way forward.

---

[1] Sections 5.4.2 Network Security Monitoring; 5.4.8 Testing and Vulnerability Management

DHS has not replicated client-side attacks or rogue tunnel audits on client PCs, however it routinely conducts audits on compromised personal computers. A representative sample of incidents that have been audited and describes the actions taken as a result of compromised systems is provided in Attachment 9.

Question 7.: Has the Department implemented a secure coding initiative? What portion of software deployed by the Department and its components have been tested using source code analysis tools? What portion of web applications have been tested using web application security tools? How many programmers working on Department applications, whether Department or contractor employees, have been trained in secure coding techniques and what skills testing was undertaken to ensure they had mastered secure coding techniques?

The Department of Homeland Security relies heavily on Commercial Off-the-shelf (COTS) systems and applications. For this reason, Department policy requires that acquisition priority be given to products certified through any one of the three following certification programs:

- The National Security Agency/National Institute of Standards and Technology, National Information Assurance Partnership Evaluation and Validation Program
- International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement
- The National Institute of Standards and Technology (NIST) Federal Information Processing Standards Validation Program

While there is currently no Department-wide secure coding initiative, this practice is addressed in a number of ways.

The DHS Common Operating Environment primarily uses Microsoft software. In FY06/07 the Department supported the Service Oriented Architecture through the use of the Microsoft.NET environment. This coding environment provides a means to produce code to protect against buffer overflows and other threat vectors that could be used to gain privileged access to computing environments.

The Federal Law Enforcement Training Center (FLETC) has limited legacy software applications and associated coding. Although the center has not used secure coding in the past, its latest Student Administration and Scheduling System (SASS), currently being developed under contract will be tested using source code analysis tools in the 3rd Quarter of FY07.

The Transportation Security Administration (TSA) is in phase one of implementing source code analysis tools, which it intends to employ on all applications, including web-enabled systems. Implementation will include appropriate training for TSA employees and contract language requiring training for contractor personnel.

Other Components, such as the National Protection and Programs Directorate (NPPD) manually check secure coding against the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) and with the .NET questionnaire. These checklists enable NPPD to ensure that coding is "hardened" in accordance with DHS IT Security Policy.[2]

The United States Citizenship and Immigration Services (USCIS) tests selected enterprise applications as part of an independent validation and verification (IV&v) process. New application code is run through a security test and evaluation (ST&E) process as part of the normal IT lifecycle management methodology.

Components who do not perform their own source code analysis are required to utilize applications and operating systems found in the DHS Technical Reference Model (TRM) database. The Customs and Border Protection (CBP) Technical Review Committee (TRC), reviews and approves software and hardware for insertion into the TRM. The TRC considers other test results, such as those conducted as part of the National Information Assurance Partnership (NIAP) testing program.

Question 8.: Has the Department mandated two-factor authentication for all privileged personnel and system administrators? If not, why not?

The Department currently employs a number of two-factor authentication technologies, including the Common Access Card (CAC) and RSA (Token-based). These technologies were implemented at the Component level and were selected to meet specific mission needs. There is currently no Department-wide solution in place, however two-factor authentication will be incorporated as part of the Department's implementation of Homeland Security Presidential Directive #12 (HSPD–12). HSPD–12 is provided in Attachment 10.

[2] Hardening in this context means the use of security configuration checklists to greatly improve overall levels of security in organizational systems; however, no checklist can permit a system or a product to become 100 % secure.

The Department's intent is to move to HSPD–12 compliant PIV cards as rapidly as possible. Cards will be required for all employees, as well as any other individual requiring access to Department's IT resources.

Question 9.: What legal requirements are the Department's hosting companies, data warehouses, software developers, or application service providers contractually obligated to regarding security? Please provide a narrative of the duties, layers of security, notification of security breaches, and timeliness of responses that the Department requires of these contractors. Is the Department able to audit/penetration test these entities to ensure that that standard of security has been met? Has the Department ever done so?

Response: The Department currently operates and maintains a total of 723 production systems:

506 Agency Systems
217 Contractor Systems

---

723 Total Systems

In addition to complying with all Federal Acquisition Regulations, the Department has published specific Homeland Security Acquisition Regulations (HSAR), in accordance with rule making authority granted when the Department was created. Contractor systems are tracked and maintained within the DHS tracking system and subject to the same rules and requirements as Government systems. The relevant sections and specific language associated with information security activities in the HSAR are included in Attachment 11.

For example, the Inspector General (IG) routinely reviews a sub-set of contractor systems as part of the annual FISMA review. The review includes test results of system controls, conducted as part of the system's Certification and Accreditation or required annual test. In addition, the IG has conducted several audits where the information systems were owned by contractors (including other Federal agencies) and where system tests were performed to evaluate the effectiveness of system controls. In developing its FY08 annual performance plan, the IG has identified additional audits that will test and evaluate controls on systems owned and/or managed on behalf of the Department by outside contractors other Federal agencies.

Question 10.: Please provide the annual budgets for the Chief Information Security Officer beginning in fiscal year 2003.

2003 Department created (no budget existed for this year)
2004 $12.5M
2005 $17.5M
2006 $15M
2007 $15M

Question 11.: How much money, in total, has the Department spent on meeting the requirements of the Federal Information Security Management Act (FISMA)? What percentage of the overall budget does that figure represent? Specifically, how did those reports lead to improved defenses against attacks? What specific changes were made? Are you confident those changes improved your defenses?

Total spending in DHS for IT security is as follows (all dollar figures are in millions):

Year	IT Security	IT Total	IT Security as % of all IT
2006	$312.3	$3811.5	8.2%
2007	$331.7	$4879.6	6.8

DHS has implemented the Federal Information Security Management Act (FISMA) through a comprehensive set of Department-specific policies that incorporate all federal guidance, including National Institute of Standards and Technology (NIST) standards and guidance, as well as Office of Management and Budget (OMB) memoranda. NIST Special Publication (SP) 800–53 is fully incorporated into Department policies and it provides the core set of controls implemented at the system level. Specifically, in 2006, the Department completed a year-long system accreditation project and the number of systems that are fully accredited rose 24% to 95%. As a result of this effort, systems now have documented plans in place for implementing the NIST recommended IT security controls, and the effectiveness of these controls has been verified for each system.

Question 12.: When the Department purchases software, do procurement documents require that the purchased software operates effectively on the secure configurations? If not, what does the Department do when a purchased package requires security configurations to be weakened in order to run the purchased application?

The Homeland Security Acquisition Regulations require vendors to comply with all Department IT security policies (specifically 4300A) including the Department's operating systems configuration guidance. (Note: The Department has published hardening guidance for all operating systems that are currently in use or that are planned for in future implementations.) Waivers to this policy expressly require risk acceptance and mitigation measures and a plan for bringing the system into compliance.

Question 13. What are your top three initiatives for securing the Department for How do you measure those goals?

The Department is currently pursing a number of initiatives to improve our overall Information Security posture. Among these, the top three are:

- 100% FISMA compliance
- Consolidated networks and datacenters
- HSPD–12 implementation

Full compliance with FISMA will allow the Department to fulfill the goals of the act, including implementing cost-effective, risk-based information security programs; providing improved, cost-effective application of IT security controls; allowing for more consistent, repeatable security control assessments; and providing more complete, reliable, and real-time information to the DHS leadership. This initiative is currently underway and being tracked through monthly FISMA Scorecards for each Component. The overall success will be realized by an increased Department-wide OMB FISMA score.

Consolidation of DHS networks and datacenters is also a top priority. The Department currently operates a number of scattered networks and datacenters of varying capabilities, making it difficult to maintain consistent standards, increasing costs and forcing duplication of effort. Consolidation will allow for improved standardization, giving the Department a greater ability to apply more effective and consistent security policies, reducing operations and maintenance costs, and allowing DHS to better focus efforts and resources. Overall success will be realized through improved security, consistent capabilities, and decreased costs.

HSPD–12 implementation is another priority. This initiative will give the Department an increased identity verification capability for its employees and contractors, allowing for tighter physical and logical access controls. Furthermore, HSPD–12 will give DHS the ability to implement two-factor authentication for all Government and Contractor personnel, as well as providing a secure, reliable interoperability capability with all other Federal agencies.

[See committee file for all attachments.]

VerDate Nov 24 2008 09:38 Aug 12, 2009 Jkt 000000 PO 00000 Frm 00051 Fmt 6601 Sfmt 6011 H:\DOCS\110-HRGS\110-52\48926.TXT HSEC PsN: DIANE